ТЕК-инжиниринг» в Гомеле. Здесь же осваивают производство умных счетчиков холодной и горячей воды.

Для создания системы KPI необходима совместная работа всех структур предприятия с обязательным привлечением главных специалистов, таких как энергетики, технологи, специалисты экономического отдела, специалисты планово-экономического отдела и других. Это является необходимым условием для создания эффективной системы KPI и, по мнению специалистов, позволят достичь экономии энергетических ресурсов на 5–7 % только за счет повышения эффективности управления комплексной системой оценки энергоэффективности.

Выбор показателей, достаточно точно оценивающих эффективность использования энергетических ресурсов на предприятии, приводит к значительным позитивным результатам. Только с помощью подробного энергоанализа есть возможность рационализировать энергопотребление на предприятии и тем самым создать качественное управление им. Таким образом, внедрение системы KPI позволит снизить энергетические затраты производства, повысить его энергоэффективность и в итоге повысить устойчивость развития предприятия в общем.

**Список использованных источников**

1. Энергомеджмент [Электронный ресурс]. – 2020. – Режим доступа: https://www.konsom.ru/solutions/informatsionnye-sistemy/sistemy-tsehovogo-energosberezheniya-ais-mes-energouchet/energomenedzhment. – Дата доступа: 07.12.2021.

2. Тыршу, М. С. Энергоаудит как инструмент энергосбережения / М. С. Тыршу // Проблемы региональной энергетики. – 2013. – № 3 (23). – С. 73–79.

3. Дырдонова, А. Н. Повышение энергоэффективности промышленного кластера региона / А. Н. Дырдонова // Сборник научных статей XV Международной научно-практической конференции молодых учёных «Развитие территориальных социально-экономических систем: вопросы теории и практики». – Екатеринбург : Институт экономики УрО РАН, 2017. – С. 129–133.

***УДК 330***

## СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

***Касевич О. А.***
***Полоцкий государственный университет, г. Новополоцк, Республика Беларусь***
***Научный руководитель: Строганова И. А., м. э. н., старший преподаватель***

Развитие цифровой экономики предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности – от утечек информации до кибертерроризма. На ранних стадиях развития сетей связи вопросы безопасности не были главными из-за небольшого количества пользователей и наличия в основном локальных сетей, в которых подразумевается доверие всех пользователей друг другу. С развитием технологий и разрастанием сетей связи выросло и значение обеспечения безопасности [1].

*Кибербезопасность* организаций финансово-банковской сферы должна базироваться на готовности подразделений безопасности противостоять новым кибератакам, понимании всего спектра угроз в отношении организации в целом и распределения приоритетов между активами организации и их защитой [2].

Пожалуй, единственный способ защитить все устройства, объединенные интернет-сетью, – это надежная защита единого центра управления интернетом вещей. Учитывая, что финансовый и банковский сектора наиболее восприимчивы к внедрению новейших достижений, приведем основные направления совершенствования кибербезопасности. (Таблица 1).

*Таблица 1 – Направления совершенствования кибербезопасности в условиях применения системы электронного банкинга и интернета вещей*

| **Направление** | **Цель** | **Что надо сделать регулятору** | **Что должны сделать банки** |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| Нормативно-правовое регулирование в области кибербезопасности | Повысить роль регулятора в вопросах кибербезопасности системы электронного банкинга и Интернета вещей | Создать орган, с функцией постоянного мониторинга кибератак на банки и оперативное реагирование на них. Разработать и внедрить регламенты взаимодействия при передаче сведений о кибератаках | Организовать выполнение регламентов взаимодействия при оперативной передаче сведений о кибератаках регулятору. Выполнять рекомендации регулятора по обеспечению кибербезопасности |
| Надежность аппаратно-программного обеспечения системы электронного банкинга | Повысить надежность аппаратно-программного обеспечения, в том числе их защищенность от кибератак | Установить требования по надежности и защищенности аппаратно-программного обеспечения системы электронного банкинга и организовать взаимодействие по данному вопросу с разработчиками системы электронного банкинга и провайдерами услуг | Внедрять аппаратно-программное обеспечение системы электронного банкинга, соответствующее требованиям по надежности и защищенности. Повысить качество заключаемых договоров с разработчиками аппаратно-программного обеспечения и провайдерами услуг |
| Финансовая грамотность населения и уровень профессиональной подготовки персонала банков | Повысить уровень финансовой грамотности населения и персонала банков по вопросам обеспечения кибербезопасности | Разработать и довести до банков рекомендации по повышению уровня финансовой грамотности клиентов и персонала по вопросам обеспечения кибербезопасности. Разработать программу и методику проведения киберучений для Национального банка Республики Беларусь и для коммерческих банков | Организовать доведение информации до клиентов банков о различных мошеннических схемах с использованием системы электронного банкинга. Постоянно проводить переподготовку персонала по вопросам кибербезопасности |

*Примечание – Источник: собственная разработка на основе [3]*

Перечисленные направления представляют далеко не полный перечень мероприятий, которые необходимо выполнить в рамках обеспечения кибербезопасности в условиях применения интернета вещей. Ведь в реальной практике каждое направление будет содержать гораздо больше задач, направленных на достижение цели.

В перспективе нужно стремиться создать *не только систему надзора* в виртуальном пространстве, но и поднять культуру поведения в нем всех участников информационного обмена. Финансовые институты должны использовать защищенные программные продукты, иметь квалифицированный обслуживающий персонал, способный оперативно и грамотно реагировать на кибератаки, а также всегда готовый прийти на помощь своим клиентам, оказавшимся в трудной ситуации.

Также стоит отметить, что одними из наиболее опасных кибератак, на которые следует бесспорно реагировать и пытаться их предотвратить, работая на опережение, являются инсайдерские угрозы.

*Инсайдерские угрозы* — это вредоносные для организации угрозы, которые исходят от людей внутри организации, таких как работники, бывшие работники, подрядчики или деловые партнеры, у которых есть информация о методах безопасности внутри организации, данных и компьютерных системах.

В данном контексте финансовые организации особенно уязвимы – они являются естественной целью, в первую очередь из-за того, что типы данных, которые они собирают, – финансовые и личные – дорого ценятся на рынке при перепродаже. Учитывая это, неудивительно, что в финансовых компаниях фиксируется больше нарушений безопасности, исходящих изнутри, чем в организациях из любого другого сектора рынка.

Почти каждый сотрудник может нести угрозу – все, что для этого требуется, это доступ к конфиденциальной информации или просто доступ к офису компании, независимо от того, работает ли человек в данной организации или нет.

Удаленные пользователи, работающие изолированно, с большей вероятностью станут жертвами атак с применением методов социальной инженерии, ведь они не могут просто пододвинутся на стуле к коллеге и спросить легитимны ли запросы злоумышленников. В условиях домашнего офиса меньше контроля и ограничений, что, к сожалению, ведет к ослаблению бдительности.

В штаб-квартире компании IT-специалисты также сталкиваются с проблемами, вызванными удаленными сотрудниками. Внешние соединения создают больше логов трафика и данных о событиях, которые необходимо анализировать, в то время как ресурсы отнюдь не бесконечны. Атака может просто затеряться в информационном шуме. Управление традиционными внутренними рисками, вероятно, уже является частью IT-стратегии любой финансовой организации.

Поэтому для эффективности мер, обеспечивающих кибербезопасность, предлагаются направления по минимизации инсайдерских угроз для финансово-банковской сферы (таблица 2).

*Таблица 2 – Рекомендации по управлению рисками инсайдерских угроз*

| **Рекомендации** | **Описание** |
|---|---|
| 1 | 2 |
| Обезопасьте удаленные соединения | Шифрование данных в реальном времени имеет важное значение, поэтому следует использовать SSL и IPSec VPN вместе со строгой аутентификацией при подключении удаленных пользователей к сети и предоставлении им доступа к данным. Сюда также входит проверка зашифрованного трафика, поскольку туннели VPN могут быть так же легко, как и легальный трафик, использованы для передачи вредоносных программ и финансовых данных без обнаружения. Это потребует развертывания межсетевого экрана, производительность которого соответствует масштабу организации. |
| Шифруйте хранимые данные | Все конфиденциальные данные, в том числе те, которые хранятся на устройствах сотрудников, должны быть зашифрованы. Если это невозможно, удаленным сотрудникам следует запретить хранить данные на личных устройствах. |
| Применяйте технологии контроля доступа | IT-командам нужны все возможные ресурсы, способные обеспечивать видимость пользователей, устройств и приложений в сети, чтобы контролировать, кто и к каким приложениям имеет доступ. Автоматический контроль доступа – важный инструмент, который необходимо взять на вооружение. |
| Считайте безопасность конечных точек приоритетной | Атаки на конечные точки весьма распространены, что обуславливает необходимость регулярной оценки устройств на предмет наличия уязвимостей и сложных угроз. Важно использовать передовые решения безопасности, такие как EDR (endpoint detection and response – система обнаружения и реагирования на угрозы конечным точкам), обеспечивающая защиту от вредоносных программ и взломов в реальном времени. Эти решения также следует сочетать с целостной структурой безопасности, которая может автоматически обнаруживать, реагировать и управлять угрозами, тем самым защищая данные, сокращая время простоя системы и обеспечивая непрерывность бизнеса. |

*Продолжение таблицы 2*

| | |
|---|---|
| Отслеживайте необычную активность | Используйте технологии SIEM и SOAR для предупреждения об аномальных попытках входа в систему, необоснованной передаче больших объемов данных или других необычных сетевых событиях. |
| Обучайте удаленных сотрудников | Сотрудники должны знать и соблюдать политики безопасности, относящиеся к удаленной работе. |

*Примечание – Источник: собственная разработка на основе [4]*

Таким образом, борьба с инсайдерскими угрозами жизненно важна для обеспечения непрерывности бизнес-процессов. Сегодня внутренние угрозы представляют беспрецедентную опасность для финансового сектора, особенно для тех организаций, которые перешли на удаленную работу для обеспечения непрерывности бизнеса. Хотя для защиты от внешних киберпреступников введены различные меры безопасности, традиционные методы не всегда учитывают угрозы, которые уже существуют внутри компании. Понимание специфики существующих внутренних угроз и выполнение рекомендаций, изложенных выше, поможет лучше защитить вашу сеть, клиентов и сотрудников от новых рисков, обусловленных стратегией удаленной работы.

**Список использованных источников**

1. Грень, И. В. Компьютерная преступность / И. В. Грень. – Минск : Новое знание, 2007. – 413 с.

2. Конявский, В. А. Компьютерная преступность: в 2-х т. / В. А. Конявский, С. В. Лопаткин. – М. : РФК-Имидж Лаб, 2006. – Т. 1. – 560с.

3. Фролов, Д. В. Обеспечение информационной безопасности в условиях ДБО / Д. В. Фролов, А. Л. Поспелов, П. В. Ревенков // Аналитический банковский журнал. – 2014. – № 6 (219). – С. 76–81.

4. Как устранить внутренние угрозы в финансовых организациях в условиях удаленной работы [Электронный ресурс]. – Режим доступа: https://www.klerk.ru/buh/articles/505467. – Дата доступа: 07.10.2020.

***УДК 330***

## ДИАГНОСТИКА РЫНКА ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РЕСПУБЛИКЕ БЕЛАРУСЬ

***Артерчук Д. Л.***
***Брестский государственный технический университет, г. Брест, Республика Беларусь***
***Научный руководитель: Кот Н. Г., старший преподаватель***

Компьютерные технологии и искусственный интеллект стремительно проникают во все сферы жизнедеятельности человека, от экономики до медицины и сельского хозяйства. Эта трансформация влечет за собой и появление новых технологий и концепций, таких как Big Data или интернет вещей. Согласно информации, изложенной в Декрете 8 Президента Республики Беларусь, с 2017 года Беларусь взяла курс на цифровизацию: предполагается, что IT-технологии должны стать одной из главных составляющих новой экономической модели [6].

На примере социальной реальности можно заметить, что посредством цифровизации происходят изменения социальных институтов (и появление новых) и их социальной организации, трансформируется социальная структура, вырабатываются новые социальные нормы и модели поведения, происходит виртуализация жизни общества и индивида.

Ввиду преимуществ, которые сегодня предоставляют цифровые технологии и создаваемые с их помощью цифровые продукты, во многих государствах реализуются масштабные проекты (например, Индустрия 4.0 в Германии, Общество 5.0 в Японии, программа Интернет+ в Китае, проекты строительства цифровой экономики в Беларуси) [2].

К флагманам цифровизации на данном этапе следует отнести следующие технологии: блокчейн (технология хранения данных, которые хранятся в цепочке последовательно свя-