Следует подчеркнуть, что произойдет рост производительности труда.

Таблица 2 – Финансовые результаты РУП «Учхоз БГСХА»

Показатели	Факт.	Расчет.	Расчет к факту,%
Выручка от реализации продукции, тыс. руб.	16146	19055,7	118,0
Себестоимость продукции, тыс. руб.	15776	17876,1	113,3
Прибыль от реализации продукции, тыс. руб.	370	1179,6	318,8
Рентабельность продукции, %	2,3	6,0	3,7 п. п.

Реализация предлагаемой программы развития РУП «Учхоз БГСХА» позволит довести размер прибыли от реализации продукции до 1179,6 тыс. руб. и увеличить рентабельность реализованной продукции – на 3,7 п.п.

Список использованных источников

1. Анализ работы и обоснование перспективной программы развития сельскохозяйственных организаций на основе эконометрических и оптимизационных моделей: рекомендации / И.В. Шафранская [и др.]. – Горки : БГСХА, 2016. – 101 с.

2. Шафранская, И.В. Системный анализ и моделирование программы развития аграрных организаций: монография / И.В. Шафранская, О.М. Недюхина, И.Н. Шафранский. – Горки: БГСХА, 2016. – 292 с.

УДК 338

Марина Свиридова
(Российская Федерация)
Научный руководитель О.В. Бондарская, к.э.н., доцент
Тамбовский государственный технический университет

ПРОФИЛАКТИЧЕСКИЕ МЕРОПРИЯТИЯ ПРОТИВОДЕЙСТВУЮЩИЕ КИБЕРПРЕСТУПНОСТИ В РОССИИ

Примерно 30 лет назад человечество даже не могло представить, что их будущее будет состоять из цифровых технологий.

Людям, что бы добыть новую информацию приходилось большое количество времени проводить в библиотеках.

Развитие человечества не стоит не месте, придумывается что-то новое. Исходя из этого, современная жизнь человека стала цифровизационной. Появились гаджеты с выходом в интернет. С его помощью стало быстрее находить нужную нам информацию, а так же отправлять различные сообщения и документы.

Мы используем интернет, даже не догадываясь о том, что в любой момент можем стать жертвами киберпреступности. Объектами киберпреступности могут быть государство, бизнес, а так же граждане.

Атаки в сторону государства могут быть направлены на государственные системы управления, масштабное отключение платёжных систем, атаки на персональные компьютеры, а так же на важную инфраструктуру государственных предприятий.

Бизнес подвергается хакерским атакам на сайты компаний, блокируются системы онлайн-торговли и т.д.

Лакомым кусочком для киберпреступников, являются обычные граждане. Ввод персональных данных может сыграть с отправителем злую шутку. Бывают случаи, что таким образом совершаются кражи денежных средств с банковских карт. Согласно отчёту ФинЦЕРТ Центробанка, за 2019 год с карт россиян увели почти 6,5 млрд. руб.

В 2020 году преступники списали с банковских карт на 70 % больше средств, чем в 2019 году.

Что бы организации не стать жертвой мошенничества, прежде всего нужно использовать эффективные технические средства защиты; хранить информацию в закрытом виде; создавать резервные копии; использовать разные учётные записи и пароли; не использовать простые пароли; не использовать пароль более 3 месяцев; контролировать безопасность систем; своевременно обновлять используемое ПО; повышать осведомлённость работников организации; проводить анализ защищённости веб-приложений; позаботиться о безопасности клиентов; повышать осведомлённость клиентов в вопросах информационной безопасности; рассказать клиентам о действиях в случае подозрения о мошенничестве; уведомлять клиентов о событиях, связанных с информационной безопасностью.

Что бы гражданам обезопасить себя от мошеннических действий нужно соблюдать ряд правил:

– не экономить на безопасности и использовать лицензионное ПО;

– на всех устройствах использовать систему антивируса;

– обновлять ПО по мере выхода патчей;

– важные данные хранить на нескольких носителях;

– отказаться от простых паролей;

– использовать разные пароли на различных системах;

– менять пароли каждые три месяца; проверять полученную информацию на электронную почту через антивирус;

– осторожно относиться к сайтам с некорректными сертификатами; быть внимательным при вводе персональных данных;

– не переходить по подозрительным ссылкам;

– не загружать файлы с подозрительных и незнакомых сайтов.

Помимо этого, важно проводить комплексную политику на государственном уровне, учитывающую взаимодействие между государствами и международными организациями, оказывающими помощь в предотвращении угроз и борьбе с недостатками в информационных технологиях.

Отдельно необходимо отметить важность повышения финансовой грамотности населения путем распространения среди граждан индивидуальных методов и способов защиты личной информации.

УДК 658.014

Анастасия Стрельченко
(Республика Беларусь)
Научный руководитель М.М. Кондровская
Белорусский государственный аграрный технический университет

МОДЕЛЬНАЯ ПРОГРАММА РАЗВИТИЯ ПРЕДПРИЯТИЯ

При изучении экономических явлений в агропромышленном производстве все более широкое применение находят экономико-математические методы.

Одно из направлений повышения эффективности АПК – совершенствование его территориальной организации, обеспечение пропорциональности во взаимодействии сельскохозяйственного и пе-