

вводить стадии уничтожения и переработки вредных побочных продуктов, использованных растворителей и других отходов, поскольку их просто не образуется. Сокращение числа стадий ведет к экономии энергии, и это тоже положительно сказывается на экологической и экономической оценке производства.

Основные направления «зеленой» химии:

- новые пути синтеза (часто это реакции с применением катализатора);
- возобновляемые источники сырья и энергии (то есть полученные не из нефти);
- замена традиционных органических растворителей.

«Зеленая» стратегия в области производства требует перехода к новой политике в обращении с химическими веществами. В 2007 г в Европейском Союзе вступило в силу новое техническое законодательство, предусматривающее регистрацию (*Registration*), оценку (*Evaluation*), разрешение (*Authorisation*) и ограничение (*Restriction*) химических веществ (*REACH*). В настоящее время более 17 белорусских предприятий, в том числе ОАО «Белшина», РУП «СПО Химволокно», прошли предварительную регистрацию в соответствии с REACH.

«Зеленая» стратегия должна коснуться и нанотехнологических производств. В настоящее время в развитии «зеленых» технологий лидирует Республика Южная Корея. Республика Беларусь находится пока в начале пути к «зеленым» технологиям, который четко обозначен в государственной стратегии устойчивого развития. Однако успехи, достигнутые, в частности, в области производства биотоплива, уже сейчас обеспечивают уверенность в достижении намеченных целей.

Литература

1. Научно-образовательный портал [Электронный ресурс] / Химия в интересах устойчивого развития. — Режим доступа: <http://www.greenchemistry.ru/popularization/golubina.htm>. — Дата доступа: 03.10.2016.
2. Поляков, М. Химия и жизнь / М. Поляков. — 2004. — № 6. — С. 8–11.
3. Устойчивое развитие Республики Беларусь на принципах «зеленой» экономики: национальное сообщение / НИЭМ М-ва экономики Респ. Беларусь. — Минск, 2012 — 53 с.

И.А. Шарко

Научный руководитель — А.Н. Иващенко

КИБЕРРИСКИ КАК НОВАЯ УГРОЗА ФИНАНСОВОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ

В статье рассмотрены киберриски в качестве новой угрозы финансовой безопасности организаций, проанализировано состояние киберпреступности в

мире и в Республике Беларусь, а также отражен способ нивелирования киберрисков посредством страхования.

Происходит цифровая трансформация бизнеса, что влечет за собой новые риски. В прошлом году ежедневно фиксировался один миллион новых киберугроз по всему миру, и это не перестает настораживать. По результатам исследования Allianz в 2016 г. киберриски впервые числятся среди трех главных глобальных бизнес-рисков. Отмечается, что по данным рискам наблюдается ежегодный интенсивный прирост, что и проиллюстрировано на рис. 1 [1].

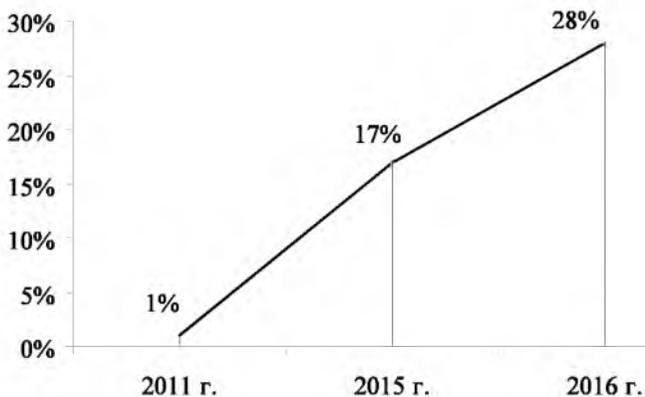


Рис. 1. Динамика киберугроз в мире

Угрозы киберрисков для финансового сектора становятся масштабнее и опаснее — 38 % преступлений в секторе финансовых услуг сегодня являются результатом именно киберпреступлений, из них 65 % кибератак осуществились по малому и среднему бизнесу. В зоне наибольшего риска находятся банки, электронные платежные системы, фондовый рынок, финансовые компании. Суммарный ущерб мировой экономике от киберпреступлений составил 445 млрд дол. США в 2015 г. Из них более 200 млрд дол. США приходится на четыре страны — США, Китай, Германию, Бразилию.

Нельзя полагать, что мировая угроза киберрисков не коснулась Республики Беларусь. В июле 2016 г. пресс-службой компании «Лаборатория Касперского» была опубликована статья об увеличении кибератак на белорусский бизнес в два раза [4]. За первые шесть месяцев 2016 г. среднестатистический рабочий компьютер в корпоративной сети белорусской организации подвергся пяти атакам вредоносного программного обеспечения, что в два раза больше, чем за предыдущий аналогичный период. На рис. 2 отражена статистика преступлений в сфере высоких технологий в Республике Беларусь в динамике с 2005 по 2015 г [3].

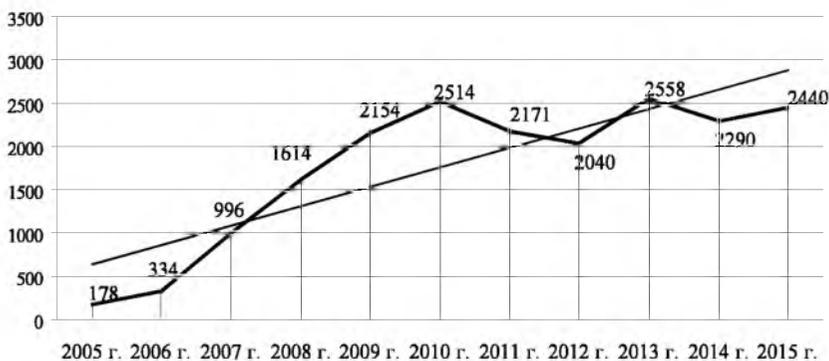


Рис. 2. Статистика преступлений в сфере высоких технологий в Республике Беларусь за 2005–2015 гг.

Отметим, что благодаря раскрытию преступлений удалось возместить 31,5 % материального ущерба, составившего в 2015 г. 69,47 млрд бел. р. (до денационации).

Одним из наиболее действенных методов снижения киберрисков видится страхование. Наибольшим успехом сейчас пользуется программа страхования киберрисков CyberEdge от American International Group, представленная в таблице [5].

Программа страхования киберрисков CyberEdge

Обязательные секции полиса		
Покрытие А	Покрытие В	Покрытие С
<p>Ответственность за нарушение персональных данных и корпоративной информации (коммерческие тайны, перечни клиентов и пр.) по причине несанкционированного раскрытия или передачи, в том числе заражения вирусами, уничтожения, модификации или удаления информации, физической кражи или утери аппаратного обеспечения и др.</p>	<p>Покрытие расходов при административном расследовании в отношении данных со стороны регулирующих органов</p>	<p>Расходы на программно-техническую экспертизу, позволяющую установить причину утечки; расходы на восстановление репутации компании и/или должностных лиц; расходы на уведомление субъектов данных и мониторинг; расходы на восстановление электронных данных</p>

Дополнительные покрытия		
Покрытие D	Покрытие E	Покрытие F
Ответственность за содержание информации	Виртуальное вымогательство	Убытки от сбоев в работе сети в результате нарушения функционирования системы безопасности, компенсация недополученной прибыли

На основе изложенного можно говорить о резком увеличении доли киберрисков в структуре бизнес-рисков, их постоянном совершенствовании, вследствие чего компаниям необходимо совершенствовать и политику своей финансовой безопасности. Аналитики делают прогнозы о предстоящем немалом увеличении спроса на услуги страхования киберрисков: по прогнозам Allianz, объемы глобального рынка страхования киберрисков превысят 20 млрд дол. к 2025 г.

В Республике Беларусь уже сложились предпосылки для возникновения страхования киберрисков, однако говорить о его самостоятельном развитии еще рано. Внедрение страхования киберрисков на данном этапе развития экономики мало представимо. Белорусский страховой рынок не готов к такому шагу. Ни одна белорусская страховая компания не осмелится взять на себя такие риски, и редко какая организация или предприятие позволит себе купить весьма недешевый пакет страхования киберрисков. Тем не менее необходимо активно следить за современной общемировой тенденцией для выработки фундамента нового, столь перспективного направления в будущем.

Литература

1. Барометр рисков Allianz 2016: С какими новыми рисками сталкиваются предприятия? [Электронный ресурс]. — Режим доступа: <http://www.allianz.ru/ru/press/news/article22443967>. — Дата доступа: 17.02.2016.
2. Число кибератак на белорусский бизнес удвоилось за последние полгода [Электронный ресурс]. — Режим доступа: http://www.kv.by/news/1048699-chislo-kiberatak-na-belorusskiy-biznes-udvoilos-za-poslednie-polgoda?utm_source=weekly_letter. — Дата доступа: 10.09.2016.
3. Управление по раскрытию преступлений в сфере высоких технологий Министерства внутренних дел Республики Беларусь [Электронный ресурс]. — Режим доступа: <http://mvd.gov.by/main.aspx?guid=1881>. — Дата доступа: 17.09.2016.
4. American International Group [Electronic resource]. — Mode of access: <http://www.aig.com/home>. — Date of access: 07.04.2016.
5. Технологии защиты информации и информационная безопасность организаций: материалы конференции. — Минск, 2016.
6. Hollmer, M. Insurance industry says cyber threat database needed [Electronic resource]//M. Hollmer//Insurance Journal. — Mode of access: <http://www.insurancejournal.com/news/national/2015/04/06/363334.htm>. — Date of access: 11.09.2016.