**А. Б. Демуськов**
*г. Гомель, ГГУ имени Ф. Скорины*

## ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ

На сегодняшний день в нашу жизнь, как на производстве, так и в быту проникают информационные технологии. И с появлением новых электронных устройств и программного обеспечения к ним появляются и информационные угрозы. Они могут проявляться как угрозы, порча и кража данных, блокировании баз данных и каналов связи вплоть до вывода из строя ресурсных серверов [1]. Для построения защиты от всевозможных информационных атак на любом предприятии должна быть построена система информационной безопасности. Под системой информационной безопасности можно понимать набор принятых управленческих решений, направленных на защиту, как самой информации, так и ресурсов с ней связанной. Как правило, систему безопасности строят на двух уровнях [2]. К первому уровню относят решения, затрагивающие предприятие в целом. Они могут носить, весьма общий характер и, как правило, должны исходить от руководства предприятия. На этот уровень выносится управление защитными ресурсами и координация использования этих ресурсов, определение специального персонала для защиты важных систем. На этом уровне система должна четко очерчивать сферу своего влияния. Должны быть определены должностные лица и их обязанности по выработке системы безопасности и по проведению ее в жизнь. В этом смысле система безопасности является основой подотчетности определённого персонала.

Ко второму уровню можно отнести вопросы отдельных аспектов информационной безопасности, но важных для различных систем, эксплуатируемых предприятием. Система должна отражать запрещённые действия и последствия за их нарушение.

Среди действий по реализации информационной безопасности в жизнь являются управленческие мероприятия.

Чтобы понять и реализовать программу информационной безопасности, ее необходимо структурировать в соответствии со структурой предприятия. В простейшем случае достаточно двух уровней: верхнего, который охватывает всю организацию, и нижнего, который относится к отдельным сервисам или группам однородных сервисов.

Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность предприятия. У этой программы должны быть определены главные цели:

– Управление рисками (оценка рисков, выбор эффективных средств защиты, и т. д.);

– Координация деятельности в области информационной безопасности;

– Стратегическое планирование;

– Контроль деятельности в области информационной безопасности.

В рамках программы верхнего уровня принимаются стратегические решения по безопасности, оцениваются технологические новинки. Информационные технологии развиваются очень быстро, и необходимо иметь четкие понятия отслеживания и внедрения новых средств.

Контроль деятельности в области информационной безопасности имеет двоякую направленность. Во-первых, необходимо гарантировать, что действия предприятия не противоречат законам. Во-вторых, нужно постоянно отслеживать состояние информационной безопасности внутри предприятия, и реагировать на все нарушения.

Так же необходимо понимать, что программа верхнего уровня должна занимать четко определенное место в деятельности предприятия, она должна официально приниматься и поддерживаться руководством, у нее должны быть определенны штаты, бюджет и определённый уровень полномочий.

Целью программы нижнего уровня является обеспечение надежной и экономичной защитой конкретных сервисов. На этом уровне решается, какие механизмы защиты использовать, закупаются и устанавливаются технические средства, выполняется повседневное администрирование, отслеживается состояние слабых мест.

Из множества возникающих рисков при выполнении мероприятий по защите интерес составляют только те, которые являются следствием использования информационных технологий [3].

Работы по управлению рисками состоят в том, чтобы оценить их размер, выработать меры по уменьшению их размера и затем убедиться, что риски приемлемы или могут быть сделаны такими.

Риски нужно контролировать постоянно. И качественно выполненная и документированная первая оценка может существенно упростить последующую деятельность.

Для небольшого предприятия допустимо рассматривать всю информационную инфраструктуру, однако, если предприятие крупное, всеобъемлющая оценка может потребовать неприемлемых затрат времени и сил. В таком случае следует сосредоточиться на наиболее важных сервисах, заранее соглашаясь с приближенностью итоговой оценки. Если важных сервисов все еще много, выбираются те из них, риски для которых заведомо велики или неизвестны.

Очень важно выбрать разумную методологию оценки рисков. Целью оценки является получение ответа на два вопроса: приемлемы ли существующие риски, и если нет, то какие защитные средства экономически выгодно использовать.

Выбирая подходящий способ защиты, необходимо учитывать возможность покрытия одним сервисом безопасности сразу нескольких и других сервисов. Важным обстоятельством является совместимость нового средства со сложившейся операционной и аппаратно-программной структурой предприятия и его подразделений.

Реализацию и проверку новых сервисов безопасности следует предварительно спланировать. Необходимо составить план тестирования, в котором учесть и наличие финансовых средств, и сроки обучения персонала. Когда намеченные меры приняты, необходимо проверить их действия и убедиться, что остаточные риски приемлемы. Если это на самом деле так, значит, все в порядке и можно спокойно намечать дату ближайшей переоценки. В противном случае придется проанализировать допущенные ошибки и провести повторный сеанс управления рисками [4].

Все эти мероприятия и есть основная часть управленческих мер обеспечения информационной безопасности.

## Список использованных источников

1 Демуськов, А. Б., Большакова, Г. И., Бышик, Т. П. Проблемы информационной безопасности в компьютерных сетях / А. Б. Демуськов, Г. И. Большакова, Т. П. Бышик // Известия Гомельского государственного университета имени Ф. Скорины. Научный и производственно-практический журнал – 2003. – №3 (18). – С. 124–129.

2 Демуськов, А. Б. Политики информационной безопасности предприятий / А. Б. Демуськов, В. А. Короткевич, Л. И. Короткевич // Известия Гомельского Госуниверситета им. Ф. Скорины. Научный и производственно-практический журнал – 2003. – №4 (19). – С. 31–36

3 Герасименко, В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк. – Москва : МИФИ, 1997. – 537 с.

4 Проблемы информационной безопасности в системе высшей школы : X Всерос. науч. конф. : сб. науч. тр. / Научная сессия МИФИ-2003 ; редкол. И. М. Ядыкин (отв. ред.) [и др.]. – Москва : Моск. инж.-физ. ин-т ( гос. ун-т), 2003. – 255 с.