УДК 004.054
DOI: 10.33764/2618-981X-2019-6-2-3-7

ОСНОВНЫЕ ПОДХОДЫ К ФОРМИРОВАНИЮ ПОЛИТИКИ БЕЗОПАСНОСТИ

Чейнеш Орлановна Оюн
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант, тел. (923)197-47-67, e-mail: cheinesh_oyun@mail.ru

Евгений Владимирович Попантонопуло
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. (909)534-23-27, e-mail: 383@2145891.ru

Игорь Николаевич Карманов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент, зав. кафедрой информационной безопасности, тел. (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

В статье отражена актуальность разработки политики информационной безопасности на предприятии, даны ключевые определения политики безопасности. Выделены основные функции, стандарты в области политики безопасности, сформулированы последствия отсутствия или некачественной разработки политики безопасности, обозначены два основных подхода к формированию политики безопасности, и раскрыта тема автоматизации процесса разработки базовой или общей политики безопасности предприятия.

Ключевые слова: политика безопасности, информационная безопасность, формирование политики безопасности, защита информации.

MAIN APPROACHES TO FORMATION OF SECURITY POLICY

Cheynesh O. Oyun
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, phone: (923)197-47-67, e-mail: cheinesh_oyun@mail.ru

Evgenij V. Popantonopulo
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Associate Professor, Department of Information Security, phone: (909)534-23-27, e-mail: 383@2145891.ru

Igor N. Karmanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Head of Department of Information Security, phone: (903)937-27-90, e-mail: i.n.karmanov@ssga.ru

In the article the relevance of information security policy development at an enterprise is shown, key definitions of security policy are given. The main functions and standards in the field of security policy are highlighted, the consequences of absence or poorly developing of security policy are formulated, two approaches to the formation of security policy are signed, and the topic of automating the process of developing of a basic or general security policy for an enterprise is disclosed.

Key words: security policy, information security, security policy formation, information protection.

Введение

В настоящее время информация, в виде отдельного ресурса, имеет ключевую значимость во многих сферах жизни человека, а также является главным ресурсом развития общества. В сфере бизнеса для любой организации информация представляет собой ценный актив, который нуждается в защите. Поэтому правильно сформированная политика безопасности (далее – ПБ) будет фундаментом для эффективной защиты информации на предприятии.

В стандарте «Оранжевая книга» приведено самое первое определение ПБ – это набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации [1].

Гостехкомиссия России определила под ПБ правила разграничения доступа, представляющие собой совокупность правил, регламентирующих правда доступа субъектов доступа к объектам доступа [2].

Также под ПБ понимают формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности [3].

Основные функции ПБ на предприятии – это соответствие актуальной нормативной базе и определение ответственности за нарушение информационной безопасности (далее – ИБ). Вследствие этого разработка ПБ – длительный и трудоемкий процесс, который требует высокого профессионализма и точных знаний нормативной базы в области защиты информации.

Методы и методики

Современная система ИБ представляет собой результат синтеза организационных и программно-технических мер, реализованных на основе единого подхода. При этом организационные меры не менее важны, чем технические – без внедрения безопасных приемов работы и осознания необходимости принимаемых мер, немыслимо создать действительно защищенную инфраструктуру безопасности.

Чтобы разработать свою ПБ, нужно четко определить цели безопасности. Цели – это конкретные шаги, которые в итоге реализуют правила ИБ. Эти шаги включают в себя обучение сотрудников и внедрение необходимого программного обеспечения, оборудования для соблюдения правил. Кроме того, когда вносятся изменения в вычислительную среду, нужно обновлять политику безопасности. Это необходимо для того, чтобы специалисты могли определить все новые риски, которые касаются нововведений [4].

Выбор нормативной базы, на которой строится разработка политики, зависит от того, в каком правовом поле и деловой среде преимущественно работает компания. Организации, привыкшие выстраивать свою деятельность на базе международных стандартов качества управления, ISO, будут готовы опираться в работе по подготовке политики информационной безопасности на такие нор-

мативные акты, как ISO/IEC 27001-2005 [5], ISO/IEC 17799-2005 [6], ISO/IECTR 13335 [7]. Российские предприятия, обеспечивающие обработку персональных данных или работающие со сведениями, содержащими государственную тайну, должны работать и с нормативами ГОСТ Р ИСО/МЭК 15408 [8].

Разработанные на их базе нормы, правила и практические приемы зададут правильный вектор на создание системы защиты от внутренних и внешних угроз, в которой обязательно будет задействована вся иерархия предприятия – от руководства до линейных сотрудников.

Структура политики безопасности выглядит следующим образом:

– определение ИБ;

– структура системы обеспечения ИБ;

– описание механизма контроля ИБ;

– оценка риска;

– безопасность информации: принципы и стандарты;

– обязанности и ответственность каждого отдела, управления или департамента в осуществлении защиты информационных носителей и прочих данных;

– ссылки на иные нормативы по безопасности.

Неправильно сформулированная ПБ или ее отсутствие в отношении государственной или коммерческой тайн или персональных данных может привести к следующим видам ущерба:

– ухудшение деловой репутации компании;

– негативное воздействие регулятора;

– отзыв лицензии или иного допуска к сведениям, которые охраняются особым образом;

– потеря клиентов, снижение интенсивности денежного потока;

– потеря собственных разработок, маркетинговых исследований, приоритета при выпуске нового продукта;

– утрата влияния на рынке, отдельных секторов рынка;

– прямые иски о возмещении вреда, вызванного утратой коммерческой тайны контрагентов, или морального вреда.

Все эти риски в финансовом плане оцениваются очень высоко. Предприниматели должны приложить все силы к разработке и внедрению работающей системы защиты конфиденциальной информации, что в дальнейшем позволит защитить свои активы от серьезного ущерба [9].

В настоящее время есть несколько подходов к формированию ПБ. Первый подход – это разделение на корпоративную и частные ПБ, где под корпоративной имеется в виду ПБ как система документированных управленческих решений по обеспечению ИБ организации, а под частными политиками или политиками по конкретным вопросам или конкретным системам подразумевают ориентированную на отдельную определенную область обеспечения ИБ или технологию, которая используется в организации. Согласно второму подходу, ПБ разделяют на две категории: организационные или административные ПБ, выполняемые людьми, и технические ПБ, которые реализуются с помощью программ и оборудования. Выбор подхода для формирования ПБ организации

осуществляется самой организацией и зависит от многих факторов, например, масштаб предприятия, состав информации, которой необходима защита, состав технических средств защиты информации [10].

Результаты

Результатом разработки политики безопасности предприятия является комплексный документ, в котором сформированы цели, задачи, принципы и способы достижения информационной безопасности. Несмотря на сложность и большой объем тем, которые должна затронуть ПБ, необходимо соблюдать следующие рекомендации:

– лаконичность – документ на 100–150 страниц, составлять которые так любят корпоративные департаменты, прочитан не будет, а значит, не будет и выполняться;

– предоставление рекомендаций максимально простым и понятным языком, где все шаги должны быть расписаны на уровне понимания простого администратора.

Рекомендуется создать документ, содержащий в себе общую политику безопасности, которую будут обязаны соблюдать все работники предприятия, и несколько локальных политик, которые будут применимы только в отдельно взятых подразделениях.

Все мы знаем, что в любой отрасли существуют аналоги, к примеру, бухгалтерские бюро на один город можно перечислять десятками. И в каждом из этих бюро есть своя концепция безопасности информации, которая, в силу своей распространенности, не будет иметь существенных отличий. Это доказывает, что не во всех случаях создание политики безопасности необходимо начинать с нуля. Зачастую можно воспользоваться существующими наработками и адаптировать типовой шаблонный комплект ПБ под свою специфику организации. Данный путь позволяет не только сэкономить многие месяцы работы, но и повысить качество разрабатываемых документов, уделяя внимание более существенным моментам. Также это является решением проблемы отсутствия на предприятии собственных ресурсов для квалифицированной разработки ПБ.

В последнее время вопрос автоматизации данного процесса является актуальным и требует тщательного анализа для дальнейшего развития. Основной идеей является создание онлайн-сайта или отдельного программного продукта, который будет содержать в себе актуальные требования и меры по защите информации, а также базу сценариев реагирования на инциденты угроз защищенности информации в организации. Структура будет такова, что ответственное лицо от организации заполняет подробную анкету-опросник, предоставляя необходимую информацию. А результатом будет являться готовый документ, который будет содержать в себе все актуальные базовые требования по защите информации, с учетом специфики организации, с отсылками к соблюденным нормативным документам, что также будет являться полезным ресурсом для экономии времени при ознакомлении и поиске необходимого нормативного документа.

Заключение

К вопросу формирования политики безопасности на предприятии необходимо отнестись с полной ответственностью. И на любом предприятии, вне зависимости от формы организации и ее масштабов, должна быть разработана и внедрена политика информационной безопасности, которая защитит предприятие от утечки информации и ее последствий. Автоматизация процесса разработки общей политики безопасности для типовых организаций решит такие проблемы, как необходимость создания особого подразделения, отсутствие времени и ресурсов, и позволит сконцентрировать внимание на особых процессах при формировании локальных или частных политик. Также сама идея автоматизации базовой политики безопасности реализуема, но требует тщательного анализа и четкой формулировки области действия для ее распространения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Department of Defense Trusted Computer System: Evaluation Criteria, DoD 5200.28-STD, 1985.

2. Рекомендации в области стандартизации Банка России РС БР ИББС-2.1 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций БС РФ требованиям СТО БР ИББС-1.0».

3. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

4. SearchInform: Цели и задачи политики информационной безопасности [Электронный ресурс]. – Режим доступа: https://searchinform.ru/products/kib/politiki-informatsionnoj-bezopasnosti/celi-i-zadachi-politiki-informacionnoj-bezopasnosti/.

5. ISO/IEC 27001-2005 «Information technology. Security techniques. Information security management systems. Requirements».

6. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью.

7. ISO/IEC TR 13335 «Information technology. Guidelines for the management of IT Security».

8. ГОСТ Р ИСО/МЭК 15408. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Введение и общая модель.

9. SearchInform: Разработка политики информационной безопасности [Электронный ресурс]. – Режим доступа: https://searchinform.ru/products/kib/politiki-informatsionnoj-bezopasnosti/razrabotka-politiki-informacionnoj-bezopasnosti/.

10. Основы управления информационной безопасностью : учеб. пособие / А. П.Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М. : НИЯУ «МИФИ», 2014. – 244 с.