Известия Гомельского государственного университета
имени Ф. Скорины, №5(32), 2005

УДК 681.3

О реализации политик информационной безопасности предприятия

А. Б. Демуськов, Т. П. Бышик, Т. Я. Каморникова

Как рассматривалось в [1], под политикой информационной безопасности мы будем понимать совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Саму политику безопасности подразделяют на три уровня. К верхнему уровню можно отнести решения, затрагивающие предприятие в целом. Они носят весьма общий характер и, как правило, исходят от руководства предприятия. Для политики верхнего уровня цели предприятия в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если предприятие отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Режимное предприятие в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности. На верхний уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем, поддержание контактов с другими предприятиями, обеспечивающими или контролирующими режим безопасности. Политика верхнего уровня должна четко очерчивать сферу своего влияния. Возможна такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы. В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и по проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

К среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных систем, эксплуатируемых предприятием. Политика должна содержать общее описание запрещенных действий и наказаний за них. Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. При формулировке целей политика нижнего уровня может ориентироваться на соображение целостности, доступности и конфиденциальности, но она не должна на них останавливаться. Ее цели должны быть конкретными.

Как только предмет политики описан, даны определения основных понятий и рассмотрены условия применения политики, надо в явной форме описать позицию предприятия (то есть решение ее руководства) по данному вопросу. Для некоторых видов политик может оказаться уместным описание, с некоторой степенью детальности, нарушений, которые неприемлемы, и последствий такого поведения.

А теперь, когда политики информационной безопасности определены, необходимы действия по реализации этих политик. Одним из основных рычагов проведение политики информационной безопасности предприятия в жизнь является управленческий.

Чтобы понять и реализовать программу информационной безопасности, ее целесообразно структурировать по уровням 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 следующие главные цели:

- управление рисками (оценка рисков, выбор эффективных средств защиты, и т.д.);
- координация деятельности в области информационной безопасности, пополнение и распределение ресурсов;

- стратегическое планирование;
- контроль деятельности в области информационной безопасности.

Управление должно быть организовано так, чтобы исключить дублирование в деятельности сотрудников предприятия, и в максимальной степени использовать знания каждого из них. Однако отсутствие дублирования, противоречит надежности, и наилучший способ защиты от потерь – это документирование накопленных знаний и освоенных процедур.

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

Контроль деятельности в области информационной безопасности имеет двоякую направленность. Во-первых, необходимо гарантировать, что действия предприятия не противоречат законам. Обязательны при этом контакты с внешними контролирующими органами. Во-вторых, нужно постоянно отслеживать состояние информационной безопасности внутри предприятия, реагировать на случаи нарушений, дорабатывать защитные меры с учетом изменения обстановки.

Необходимо отметить, что программа верхнего уровня должна занимать четко определенное место в деятельности предприятия, она должна официально приниматься и поддерживаться руководством, у нее должны быть определены штаты, бюджет и уровень полномочий. Без подобной поддержки распоряжения "службы безопасности" останутся пустым звуком.

Цель программы нижнего уровня – обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне решается, какие механизмы защиты использовать, закупаются и устанавливаются технические средства, выполняется повседневное администрирование, отслеживается состояние слабых мест. Как правило, за программу нижнего уровня отвечают администраторы сервисов. Программа безопасности не должна превращаться в набор технических средств, встроенных в систему – иначе она потеряет независимость и как следствие авторитет и высшее руководство забудет про нее и перестанет выделять ресурсы.

Деятельность любого предприятия подвержена множеству рисков. Нас интересуют только те, которые являются следствием использования информационных технологий. 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. Таким образом, управление рисками включает в себя два вида деятельности:

- оценку (измерение) рисков;
- выбор эффективных и экономичных защитных рычагов.

Процесс управления рисками можно подразделить на следующие этапы:

1. Выбор анализируемых объектов и степени детальности их рассмотрения;
2. Выбор методологии оценки рисков;
3. Идентификация активов;
4. Анализ угроз и их последствий, определение слабых мест в защите;
5. Оценка рисков;
6. Выбор защитных мер;
7. Реализация и проверка выбранных мер;
8. Оценка остаточного риска.

Этапы 6 и 7 относятся к выбору защитных рычагов, остальные – к оценке рисков.

Уже перечисление этапов показывает, что управление рисками – процесс циклический. Риски нужно контролировать постоянно, периодически проводя их переоценку. И качественно выполненная и тщательно документированная первая оценка может существенно упростить последующую деятельность.

Выбор анализируемых объектов и степени детальности их рассмотрения – первый шаг в оценке рисков. 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.

При идентификации активов, то есть тех ценностей, которые предприятие пытается защитить, следует, конечно, учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, такие как репутация предприятия. Тем не менее, одним из главных результатов процесса идентификации активов является получение детальной информационной структуры организации и способов ее использования.

Первый шаг в анализе угроз – их идентификация. Анализируемые виды угроз следует выбрать из соображений здравого смысла и в пределах выбранных видов провести максимально полное рассмотрение. Целесообразно выявлять не только сами угрозы, но и источники их возникновения – это поможет в выборе дополнительных средств защиты.

После идентификации угрозы необходимо оценить вероятность ее осуществления. Кроме вероятности осуществления, важен размер потенциального ущерба. Оценивая тяжесть ущерба, необходимо иметь в виду не только непосредственные расходы на замену оборудования или восстановление информации, но и более отдаленные, такие как подрыв репутации, ослабление позиций на рынке и т.п. После того, как накоплены исходные данные и оценена степень неопределенности, можно переходить к обработке информации, то есть собственно к оценке рисков. Если какие-либо риски оказались недопустимо высокими, необходимо реализовать дополнительные защитные меры. Как правило, для ликвидации или сглаживания слабости, сделавшей реальной некую угрозу, существует несколько механизмов безопасности, отличающихся эффективностью и стоимостью. Оценивая стоимость защитных мер, приходится, разумеется, учитывать не только прямые расходы на закупку оборудования и(или) программ, но и расходы на внедрение новинки и, в частности, на обучение и переподготовку персонала.

Выбирая подходящий способ защиты, целесообразно учитывать возможность экранирования одним сервисом безопасности сразу нескольких прикладных сервисов. Важным обстоятельством является совместимость нового средства со сложившейся операционной и аппаратно-программной структурой, с традициями предприятия.

Как и всякую иную деятельность, реализацию и проверку новых регуляторов 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 действенность, то есть убедиться, что остаточные риски стали приемлемыми. 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 немедленно.

Такова основная часть управленческих мер обеспечения информационной безопасности.

Abstract. Control actions of information safety performance is considered in the article.

Литература

1. А. Б. Демуськов, В. А. Короткевич, Л. И. Короткевич, *Политики информационной безопасности предприятий*, Известия Гомельского Госуниверситета им. Ф. Скорины. № 4 (19) (2003).

2. А. Б. Демуськов, Г. И. Большакова, Т. П. Бышик, *Проблемы информационной безопасности в компьютерных сетях*, Известия Гомельского Госуниверситета им. Ф. Скорины. № 3 (18) (2003).

3. В. А. Герасименко, А. А. Малюк, *Основы защиты информации*, Москва, МИФИ, 1997.

4. *Научная сессия МИФИ-2003*, X всероссийская научная конференция «Проблемы информационной безопасности в системе высшей школы», Сборник научных трудов, Москва, МИФИ, 2003.

5. *Гостехкомиссия России*. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации, Москва, 1992

6. В. Гайкович, А. Першин, *Безопасность электронных банковских систем*, Москва, Единая Европа, 1994.

Гомельский государственный
университет им. Ф. Скорины

Поступило 27.06.05