Балановская А.В.
Концептуальный подход к построению системы информационной безопасности промышленного предприятия // Вестник Самарского государственного университета. 2015. № 5 (127). С. 14–20

УДК 65.012.45

А.В. Балановская*

КОНЦЕПТУАЛЬНЫЙ ПОДХОД К ПОСТРОЕНИЮ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

В статье приводятся структура и содержание целей информационной безопасности промышленного предприятия, принципы проектирования и функционирования системы информационной безопасности. Выявляются основные этапы построения такой системы, анализируется их содержание.

Ключевые слова: информация, информационная безопасность, информационная система, последовательность, информационные угрозы, система информационной безопасности.

В современном мире проблема защиты информации от нежелательных воздействий стоит не только тогда, когда собственник информации не желает ею делиться по каким-либо причинам, но и в процессе ежедневной, текущей работы предприятия в стандартных условиях. К сожалению, на сегодняшний день угрозы и нежелательные воздействия на информационную систему промышленного предприятия осуществляются гарантированно в процессе использования информационных сетей, Интернета, передачи информации при помощи различных носителей и т. д. В связи с этим перед собственниками стоит проблема обеспечения информационной безопасности организационных систем. При принятии управленческих решений в процессе проектирования системы безопасности ведущим является процесс целеполагания. Он означает, что необходимо определится с целями, которые ставит перед собой информационная безопасность, и убедиться, что они соответствуют целям собственника в процессе проектирования системы безопасности.

Многие исследователи сходятся во мнении, что цели информационной безопасности можно определить двумя аспектами: во-первых, это гарантирование целостности компьютерных данных, а также программного обеспечения и технологий, обеспечивающих обработку информации, во-вторых – обеспечение конфиденциальности информации, относящейся к критичной, которая также включает и программное обеспечение, и технологии ее обработки и защиты.

Анализ этого подхода позволяет сделать вывод, что основная цель – система защиты данных в информационной системе, однако не менее важным является аспект обеспечения доступа авторизованных пользователей.

На наш взгляд, основная цель защиты информации может быть сформулирована как гарантирование конфиденциальности информации и достижение устойчивого функционирования информационной системы в процессе ее эксплуатации.

Систему информационной безопасности можно представить в иерархическом виде, предполагающем переход от частного к общему. Так, на первом уровне выделяют обеспечение безопасности ресурсов отдельно взятой информационной си-

Балановская Анна Вячеславовна (balanovskay@mail.ru), кафедра экономики промышленности, Самарский государственный экономический университет, 443086, Российская Федерация, г. Самара, ул. Советской Армии, 141.

стемы, связанной с физической и логической целостностью и доступностью. Второй уровень предполагает обеспечение технологической и организационной целостности информационной системы, различных объектов управления, партнеров и т. д. На третьем уровне базируется информационная безопасность общества и государства. При проектировании системы информационной безопасности следует учитывать цели, заявленные на первом и втором уровне.

Структура и содержание целей информационной безопасности взаимосвязаны с различными угрозами безопасности, а также с существующими средствами и методами ее обеспечения.

В организационных системах коммерческой направленности, в отличие от государственных, собственнику принадлежит полное право выбора методов, средств и мероприятий по обеспечению информационной безопасности. Для помощи собственникам в государстве формируется и совершенствуется нормативно-законодательная база, которая на методологическом уровне оказывает поддержку предпринимателям, а также правовую поддержку в организации защитных мероприятий.

Можно существенно расширить подход и поставить максимально широко задачи комплексной защиты информации в информационных системах, рассматривая следующие аспекты:

– комплексность целевая – защита по всей существующей совокупности различных показателей защищенности информации, а также всей совокупности факторов, которые влияют на защищенность;

– комплексность временная – непрерывная защита во все время и на всех этапах жизненного цикла информационной системы;

– комплексность концептуальная – исследование и реализация проблем защиты в совокупности проблем развития, построения и использования информационной системы.

Предлагается расширить содержание целевой комплексности следующими компонентами:

– обеспечение логической, а также физической целостности системы формирования информационных ресурсов и достижение их достаточной для соответствующего применения полноты, достоверности, непротиворечивости, актуальности и юридической состоятельности; логической и физической целостности применяемых технологий обработки информации, прежде всего использующих современные системы и средства информатизации; гарантий конституционных прав и свобод граждан в информационной сфере;

– предотвращение использования информационных ресурсов в ущерб правам и свободам граждан, законным интересам юридических лиц, государства и общества (предупреждение несанкционированного получения, модификации и распространения информации, а также отказа от своих действий);

– восстановление физической, логической, организационно-технологической целостности и устранение экономических потерь;

– наказание нарушителей.

Целями системы информационной безопасности являются не только предупреждение и обеспечение защиты информации, но и восстановление ее нормальной работы, а также установление и изучение причин, наказание виновных.

Функция восстановления является одной из самых главных, она должна обеспечить нормальное функционирование информационной системы, и при ее проектировании это должно учитываться.

На структуру целей влияет множество факторов, являющихся угрозами безопасности информационной системы. Цели комплексной защиты достигаются только при

взаимодействии множества средств, представляющих собой единое логическое целое, призванное обеспечить работу информационной системы в заданных режимах.

В основу проектирования и функционирования систем безопасности информации должен быть положен ряд основных принципов, выделяющихся различными исследователями [2; 3] (см. табл.).

Таблица

Принципы проектирования и функционирования системы информационной безопасности

Принцип	Содержание
Принцип законности	Необходимость строго следовать положениям соответствующего нормативно-правового обеспечения
Принцип комплексности	Блокирование всех возможных разноплановых угроз и обеспечение полноты защиты и полноты применяемых методов
Принцип минимальной достаточности	Заданная степень защиты информации, наличие разработанных требований при заданной степени риска и соответствующий этим параметрам набор средств, способных обеспечить выполнение данного комплекса требований
Принцип обоснованности	Обеспечение доказательной базы в процессе установления степени защиты и выдвигаемых требований, а также при оценке риска возможного нарушения системы защиты информационного ресурса
Принцип тактической организации защиты	Возможная система превентивных действий в виде недопущения отрицательных последствий
Принцип непрерывности состояний во времени и пространстве	Ограничение функционирования объекта вплоть до невозможности его функционирования в случае исключения защиты и обоснование необходимости резервирования систем защиты

По нашему мнению, к рассмотренным принципам следует добавить принцип восстановления нормальной работы, предполагающий обеспечение восстановления нормальной работы информационной системы предприятия в случае реализации угрозы.

В большинстве работ подходы к проектированию информационной системы предприятия и обеспечению безопасности ее функционирования сводятся к нескольким этапам, которые целесообразно рассмотреть отдельно.

В первую очередь следует провести аналитическое исследование существующей системы информационной безопасности промышленного предприятия с целью выявления возможных уязвимостей, которые несут в себе риск обрабатываемой конфиденциальной информации, и выработки необходимых требований по ее защите.

Далее следует этап проектирования системы защиты информации промышленного предприятия. В процессе его выполнения следует установить минимально приемлемые требования по защите информации от несанкционированного доступа, учитывающие условия работы информационной системы предприятия. Ограничителями на данном этапе являются выдвинутые руководством предприятия лимиты на финансовые, материальные, трудовые и другие ресурсы. С учетом этих факторов возможно осуществить выбор и дальнейшую разработку конкретных методов и средств защиты. Итогом выполнения данного этапа становится завершенный комплекс сертифицированных средств и методов защиты информации, который дополнен необходимыми проектными и эксплуатационными документами.

На третьем этапе осуществляется приемка системы в эксплуатацию. Соответствующими службами ведется внедрение средств и методов системы защиты ин-

формации в информационной системе, их тестирование и комплексная проверка, проводится обучение персонала и освоение им нововведений. На данном этапе, безусловно, наблюдается выявление различных недостатков, которые должны в реальном времени устраняться. Итогом данного этапа становится общая аттестация системы защиты информации.

Заключительный этап – этап эксплуатации системы информационной безопасности промышленного предприятия. В процессе его реализации проводится регулярный контроль эффективности, при необходимости осуществляется доработка системы, вызванная изменениями состава аппаратных средств, программного обеспечения, а также оперативной обстановки и внешнего окружения информационной системы предприятия. Важным является контроль и анализ состава информационной системы, ее структуры. Если какая-либо модификация информационной системы снижает эффективность ее функционирования, то данная модификация отклоняется.

В процессе изменения нормативно-технических требований и характеристик проводится оценка соответствия функционирующей информационной системы действующим требованиям.

По нашему мнению, исходя из проведенного анализа можно предложить последовательность построения системы информационной безопасности предприятия в несколько этапов, которые следует проработать более детально.

На первом этапе, подготовительном, происходит выбор объекта, который может быть заявлен как информационная система в целом или ее отдельная подсистема, компонент и т. д. Проводится комплексный анализ имеющихся ресурсов, выявляются ограничения, исследуются методы подготовки, приема-передачи и обработки информации, изучаются особенности архитектуры информационной системы, характер и ценность информации, обращающейся в информационной системе предприятия.

Одновременно приводится описание ресурсов системы, которые следует объединить в несколько категорий, таких как вычислительная и коммуникационная техника, программное обеспечение, данные, персонал, дополнительные ресурсы.

На основании проведенного исследования в рамках подготовительного этапа разрабатывается общая концепция системы информационной безопасности промышленного предприятия. На данном уровне следует определить цели и задачи, сформировать основополагающие требования, которые будут учитывать не только результаты анализа текущей ситуации, но и возможные перспективы развития потребностей, направления прогресса в сфере информатизации, новинки в области технологий обработки, хранения, обновления и передачи данных.

Далее планомерно осуществляется переход от подготовительного этапа ко второму этапу – аналитическому. Его основными задачами являются изучение и количественное оценивание рисков, выявление и систематизация возможных угроз, поиск возможных каналов несанкционированного доступа и утечки информации, сбор информации об объектах, подлежащих защите, а также разработка обоснованных критериев эффективности защиты информации.

При исследовании угроз, возможных и потенциальных, важно изучать информацию, поступающую из внешней среды, оценивать ее достоверность и определять степень ее полноты. Такая проверка на достоверность включает оценку различных источников информации, как первичных, так и вторичных. Изучаются периодические издания, научные конференции, специализированные публикации и т. д. Во внимание принимается также внутренняя информация, касающаяся возможных сообщений о конфликтах, сбоях и задержках, которые регистрируются информационной системой предприятия.

С учетом того, что угроза может переходить из категории «возможная» в категорию «потенциальная», необходимо оценить привлекательность реализации конкретной угрозы (или класса угроз) для потенциального нарушителя.

Важным является решение вопроса об определении критериев эффективности системы информационной безопасности, к которым можно отнести технические, экономические, социальные, критерии эффективности управления.

Изучение характеристик существующих аппаратно-программных средств защиты позволяет определиться, какие из имеющихся вариантов удовлетворяют разработанным критериям информационной безопасности. Выбираются и системы шифрования, которые будут использоваться в процессе обработки, приема-передачи, хранения и обновления информации в системе. Как показывает практика, чем больше охват рассматриваемых систем и разнообразие применяемых методов, тем, соответственно, надежнее будет функционировать вся система информационной безопасности промышленного предприятия. Однако, выбирая из разнообразия применяемых технологий, методов и средств, не стоит забывать о проблеме совместимости их с функционирующей системой (в том числе аппаратной частью, операционной системой, прикладными программами).

Исследовательский этап предполагает разработку политики безопасности, определение допустимой степени риска, набора процедур и методов исключения несанкционированного доступа к ресурсам информационной системы предприятия и т. д. Для этого разрабатываются специальные оценочные шкалы допустимых потерь, учитывающие потери как в натуральном, так и в денежном эквивалентах. Следует отметить, что потребуется разнообразие оценочных шкал, т. к. в каждой информационной системе, подсистеме и т. д. существует граница «допустимости» потерь, которая определяется ценностью хранимой информации, масштабами разработок, бюджетом и множеством других экономических, организационных, политических, морально-этических и других факторов.

В том случае, если расчетные потери меньше, чем потребные затраты на разработку, последующее внедрение и эксплуатацию средств защиты, и с точки зрения интересов информационной системы потенциально возможный несанкционированный доступ не приведет к существенным сбоям и изменениям в работе, то такой риск следует считать допустимым. При этом нужно учитывать, что в большинстве случаев целесообразно исключить даже незначительную утечку информации, например, когда речь идет о содержании конфиденциальной информации, связанной с анализом конъюнктуры рынка, новых технологий, стратегий развития, планов и бюджетов.

В проведении исследовательского этапа наиболее ответственными являются работы, связанные со сложностью разработки и принятия политики безопасности. В общепринятом смысле под политикой безопасности понимают систему правил, законов, практических рекомендаций и процедур, которую используют как основу управления, защиты и распределения критической информации в информационной системе промышленного предприятия. Прорабатываемая политика безопасности должна охватывать все особенности процесса обработки информации, с большой долей вероятности определять возможное поведение системы в различных ситуациях.

Немаловажным моментом является проработка различных серьезных механизмов обнаружения возможных попыток несанкционированного доступа к защищаемым ресурсам. Данные механизмы могут базироваться на экспертных системах. Они также должны включать распознавание, регистрацию и обработку событий, связанных с несанкционированным доступом к информации, и проводить проверку соответствия условий доступа, принятых в разработанной концепции системы информационной безопасности промышленного предприятия и защиты его данных.

В случае наступления негативных последствий несанкционированного доступа в рамках данного этапа также предусмотрена разработка плана восстановления и обеспечения нормальной работы информационной системы.

Следует отметить, что такие этапы, как аналитический и исследовательский, могут быть логически объединены в один общий этап, основной задачей которого является изучение рисков.

Этот момент регулируется особенностями информационной системы каждого отдельно взятого промышленного предприятия.

На основе полученного результата проработки возможных угроз будет создан комплекс контрмер и мероприятий, обеспечивающих необходимый и достаточный уровень защищенности информационной системы предприятия.

Испытательный этап включает в себя исследование различных вариантов размещения элементов системы информационной безопасности, выбор оптимального решения, основанного на соотношении «эффективность–стоимость», тестирование, документирование, оформление итоговых рекомендаций к внедрению.

После того как сделан выбор по критериям «эффективность–стоимость» и проведен комплекс работ, связанных с размещением элементов системы информационной безопасности в узлах информационной системы, анализируются полученные результаты. Для гарантирования устойчивости системы информационной безопасности при реализации различного рода атак проводят ее тестирование с использованием функциональных тестов. На основе отчета о тестировании может быть принято решение об использовании модулей системы информационной безопасности, в случае получения неудовлетворительного результата принимается решение о доработке либо замене того или иного модуля. Важным шагом является расчет ожидаемого эффекта от внедрения конкретной системы информационной безопасности, на основе которого может быть принято управленческое решение об использовании либо доработке конкретной конфигурации системы информационного обеспечения промышленного предприятия.

Заключительным шагом в рамках испытательного этапа является документирование, состоящее в разработке пакета методических, инструктивных, технологических материалов, которые подробным образом описывают структуру и принципы функционирования системы информационной безопасности, способы и механизмы реализации ее возможностей, план восстановления ресурсов информационной системы в случае наступления негативных событий и т. д.

Этап внедрения и технической поддержки будет включать уже непосредственно работы по внедрению и вводу системы информационной безопасности в эксплуатацию с последующим обучением и аттестацией персонала. На данном этапе также предусматриваются дальнейшее развитие и поддержка системы информационной безопасности на должном уровне, проведение регулярного тестирования на протяжении всего жизненного цикла системы с целью выявления новых видов угроз, которые не были предусмотрены разработчиками при ее проектировании, разработке и внедрении.

Своевременная модификация и развитие отдельных компонентов может осуществляться исключительно на основе полученной актуальной информации о новых угрозах и каналах утечки информации.

Считаем, что рассмотренный подход к построению системы информационной безопасности способен помочь руководителям промышленных предприятий при проведении организационных работ по проектированию системы информационной безопасности. Не следует забывать, что успешное и эффективное управление системой информационной безопасности возможно при использовании научных

методов при разработке концепции безопасности предприятия. Систему безопасности необходимо рассматривать не только как инструмент, обеспечивающий защиту деятельности, но и как важнейший ресурс и гарант успешного развития.

Библиографический список

1. Герасименко В.А., Малюк А.А. Основы защиты информации. М.: МИФИ, 1997. 537 с.

2. Домарев В.В. Безопасность информационных технологий. Системный подход. К.: Диасофт, 2004. 992 с.

3. Разработка систем информационно-компьютерной безопасности / В.М. Зима [и др.]. СПб.: ВКА им. А.Ф. Можайского, 2003. 327 с.

4. Мецатунян М.В. Некоторые вопросы проектирования комплексных систем защиты информации // Безопасность информационных технологий. 1995. № 1. С. 53–54.

5. Петров В.А., Пискарев А.С., Шеин А.В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах. М.: МИФИ, 2000. 84 с.

References

1. Gerasimenko V.A., Malyuk A.A. Information security bases. M., MIFI, 1997, 537 p. [in Russian].

2. Domarev V.V. Security of information technologies. System approach. Kiev, OOO TID «Diasoft», 2004, 992 p. [in Russian].

3. Zima V.M., Kotukhov M.M., Lomako A.G., Markov A.S., Moldovyan A.A. Development of systems of information and computer safety. SPb., VKA im. A.F. Mozhaiskogo, 2003, 327 p. [in Russian].

4. Metsatunyan M.V. Some questions of design of complex systems of information security. *Bezopasnost informatsionnykh tekhnolohgyi* [Safety of information technologies], 1995, no. 1, pp. 53–54 [in Russian].

5. Petrov V.A., Piskarev A.S., Shein A.V. Information security. Information security from unauthorized access in the automated systems. M., MIFI, 2000, 84 p. [in Russian].

A.V. Balanovskaya*

CONCEPTUAL APPROACH TO THE CONSTRUCTION OF THE SYSTEM OF INFORMATIONAL SECURITY OF AN INDUSTRIAL ENTERPRISE

The structure and maintenance of the purposes of information security of an industrial enterprise, the principles of design and functioning of an information security system is given in article. The main stages of creation of an information security system come to light, their contents is analyzed.

Key words: information; information security; information system; sequence; information threats; information security system.

* *Balanovskaya Anna Vyacheslavovna* (balanovskay@mail.ru), Department of Industrial Economics, Samara State University of Economics, 141, Sovetskaya Armiia Street, Samara, 443086, Russian Federation.