УДК 004.056

МЕТОДИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В. В. Шишкин, М. К. Танатов, Н. К. Юрков

Главной целью любой информационной безопасности является обеспечение устойчивого функционирования объекта, предотвращение угроз его функционирования, защита законных интересов от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной производственной деятельности всех подразделений объекта и др. [1–3].

Достижение заданных целей возможно при решении ряда задач:

– отнесение информации к категории ограниченного доступа (служебной тайне);

– прогнозирование и своевременное выявление угроз безопасности информационным ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;

– создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;

– создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;

– создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения информационной безопасности на достижение стратегических целей.

Абстрактная модель взаимодействия элементов информационной безопасности, в том числе и нарушителей, показана на рис. 1.

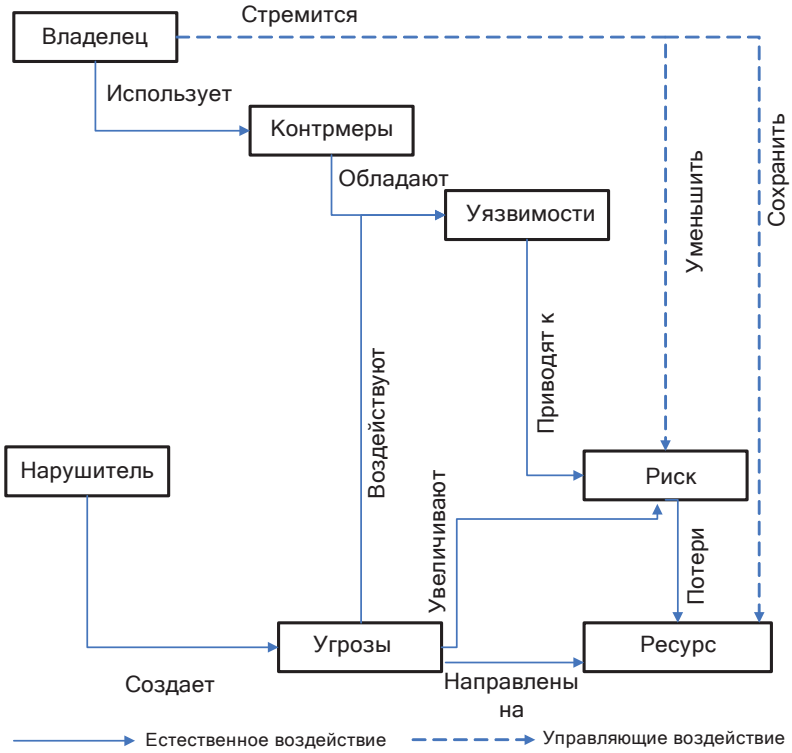

Рис. 1. Модель взаимодействия элементов информационной безопасности

Представленная модель информационной безопасности – это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов [4].

Рассматриваются следующие объективные факторы:

– угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;

– уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;

– риск-фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери – прямые или косвенные).

Для обеспечения сбалансированной информационной безопасности необходимо сначала провести анализ рисков в области информационной безопасности, затем определить оптимальный уровень риска для организации на основе заданного критерия. Таким образом, станет возможно [5–7]:

– полностью проанализировать и документально оформить требования, связанные с обеспечением информационной безопасности;

– избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков;

– оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем;

– обеспечить проведение работ в сжатые сроки;

– представить обоснование для выбора мер противодействия;

– оценить эффективность контрмер, сравнить различные варианты контрмер.

Для адекватной оценки использования ресурсов при обеспечении информационной безопасности необходимо знать, от чего конкретно будет осуществляться защита. Таким образом, необходимо провести анализ рисков, угрожающих предприятию. В этом процессе возможна следующая методология:

– описание объекта и существующих мер защиты;

– идентификация используемых ресурсов и оценивание их количественных показателей (определение потенциального негативного воздействия на бизнес);

– анализ угроз информационной безопасности;

– оценивание найденных уязвимостей;

– оценивание существующих и предполагаемых средств обеспечения информационной безопасности;

– оценивание рисков.

Риск характеризует опасность, которой может подвергаться система и использующая ее организация, и зависит:

– от показателей ценности ресурсов;

– вероятностей нанесения ущерба ресурсам (выражаемых через вероятности реализации угроз для ресурсов);

– степени легкости, с которой уязвимости могут быть использованы при возникновении угроз (уязвимости системы защиты).

Расчет этих показателей выполняется на основе математических методов, имеющих такие характеристики, как обоснование и параметры точности метода. Оценку рисков и анализ угроз можно проводить на основе предлагаемой модели (рис. 2).

Обеспечение повышенных требований к информационной безопасности предполагает соответствующие мероприятия на всех этапах жизненного цикла информационной системы. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Прежде чем предлагать какие-либо технические решения по информационной безопасности объекта, предстоит разработать для него политику безопасности.

Собственно организационная политика безопасности описывает порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности.

Рис. 2. Возможная модель оценки информационных рисков

Информационной безопасность объекта окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот. Шагами построения организационной политики безопасности можно считать:

– внесение в описание объекта автоматизации структуры ценности и проведение анализа риска;

– определение правил для любого процесса пользования конкретным видом ресурса объекта автоматизации, имеющим конкретную степень ценности.

Организационная политика безопасности оформляется в виде отдельного документа, который согласовывается с заказчиком.

Описанная методика позволяет оценить или переоценить уровень текущего состояния информационной безопасности предприятия, выработать рекомендации по обеспечению (повышению) информационной безопасности предприятия, снизить потенциальные потери предприятия или организации путем повышения устойчивости функционирования корпоративной сети, разработать концепцию и политику безопасности предприятия, а также предложить планы защиты конфиденциальной информации предприятия, передаваемой по открытым каналам связи, защиты информации предприятия от умышленного искажения (разрушения), несанкционированного доступа к ней, ее копирования или использования.

Список литературы

1. Гуревич, И. М. Информационные характеристики физических систем / И. М. Гуревич. – М. : ИПИ РАН, 2009. – 170 с.
2. Гуревич, И. М. Законы информатики – основа строения и познания сложных систем / И. М. Гуревич. – 2-е изд., уточн. и доп. – М. : ТОРУС ПРЕСС, 2007. – 400 с.
3. Крупин, В. П. Методика оценки информационных ресурсов / В. П. Крупин, Е. Е. Крупина, В. В. Лещинский. – М. : РАО, 2002. – 22 с.
4. Урсул, А. Д. Отражение и информация / А. Д. Урсул. – М. : Мысль, 1973. – 231 с.
5. Юрков, Н. К. К проблеме обеспечения безопасности сложных систем / Н. К. Юрков // Надежность и качество : тр. Междунар. симп. : в 2 т. / под ред. Н. К. Юркова. – Пенза : Изд-во ПГУ, 2011. – Т. 1. – С. 104–106.
6. Юрков, Н. К. К проблеме обеспечения глобальной безопасности / Н. К. Юрков // Надежность и качество : тр. Междунар. симп. : в 2 т. / под ред. Н. К. Юркова. – Пенза : Изд-во ПГУ, 2012. – Т. 1. – С. 6–8.
7. Грущанский, В. А. О формализации показателей эффективности и безопасности комплексных программ в условиях неопределенности и риска / В. А. Грущанский, Н. К. Юрков // Надежность и качество сложных систем. – 2013. – № 2. – С. 3–9.

УДК 004.056

Шишкин, В. В.

Методика обеспечения информационной безопасности / В. В. Шишкин, Н. К. Юрков, Н. Ж. Мусин // Надежность и качество сложных систем. – 2013. – № 4. – С. 9–13.

Шишкин Вячеслав Вячеславович
аспирант,
кафедра конструирования
и производства радиоаппаратуры,
Пензенский государственный университет
(440026, Россия, г. Пенза, ул. Красная, 40)
E-mail: d.m.00@mail.ru

Юрков Николай Кондратьевич
доктор технических наук, профессор,
заведующий кафедрой,
кафедра конструирования
и производства радиоаппаратуры,
Пензенский государственный университет
(440026, Россия, г. Пенза, ул. Красная, 40)
(8412) 56-43-46
E-mail: yurkov_NK@mail.ru

Мусин Нариман Жапарович
начальник,
Военный институт Сил воздушной обороны
им. Дважды Героя Советского Союза
Талгата Бегельдинова
(Казахстан, г. Актобе,
проспект Алии Молдагуловой, 16)

Shishkin Vyacheslav Vyacheslavovich
postgraduate student,
sub-department of radio equipment
design and production,
Penza State University
(440026, 40 Krasnaya street, Penza, Russia)

Yurkov Nikolay Kondrat'evich
doctor of technical science, professor,
head of sub-department of radio equipment
design and production,
Penza State University
(440026, 40 Krasnaya street, Penza, Russia)

Musin Nariman Zhaparovich
head,
Military Institute of Air Defense
named after Hero of the Soviet Union
Talgat Begeldinova
(16 Alii Moldagulovoy avenue, Aktobe, Kazakhstan)

Аннотация. Рассматривается методика создания и оценки системы информационной безопасности, рассматриваются подходы к оценке рисков и методов их сокращения.

Ключевые слова: информация, безопасность, риски, угрозы, нарушитель, защита.

Abstract. This article describes a technique for creating and evaluating information security systems, discusses approaches to risk assessment and methods to reduce them.

Key words: information, security, risks, threats, intruder protection.