УДК 004.056

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ, ЗАНИМАЮЩЕГОСЯ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ И ПРОИЗВОДСТВЕННОЙ ДЕЯТЕЛЬНОСТЬЮ

И. Р. Кикоть

Донской государственный технический университет, Ростов-на-Дону, Российская Федерация

kikivan7@yandex.ru

Работа посвящена анализу угроз информационной безопасности предприятия, занимающегося научно-исследовательской и производственной деятельностью. На основе изучения области деятельности, структуры предприятия, анализа возможных угроз и каналов утечки информации была выполнена классификация подлежащих защите сведений; выделены ценные объекты и ресурсы, утеря или порча которых может принести ущерб предприятию; построена схема причинно-следственных связей угроз информационной безопасности; разработана модель объекта защиты с указанием направления действия угроз информационной безопасности и дестабилизирующих факторов.

Ключевые слова: информационная безопасность предприятия, системы защиты информации, угрозы информационной безопасности, каналы утечки информации, модель защиты

UDC 004.056

ANALYSIS OF INFORMATION SECURITY THREATS OF ENTERPRISES ENGAGED IN RESEARCH AND PRODUCTION ACTIVITIES

I. R. Kikot

Don State Technical University Rostov-on-Don, Russian Federation

kikivan7@yandex.ru

This paper analyzes information security threats of an enterprise engaged in research and production activities. On the basis of the field of activity, enterprise structure, the analysis of the potential threats and information leakage channels the classification of information that should be protected was carried out; valuable objects and resources were singled out, the loss or damage of which may cause damage to the enterprise. The author has created the scheme of the cause-effect relationship of information security threats; designed a model of the object of protection with an indication of the action direction of information security threats and destabilizing factors.

Keywords: enterprise information security, information security systems, information security threats, information leakage channels, information security model

Введение. Последствиями реализации угроз информационной безопасности могут быть экономический ущерб, экологические катастрофы и даже гибель людей [1]. Совокупность задач, решаемых для обеспечения информационной безопасности и защиты информации в современных системах обработки и передачи данных, достаточно обширна [2]. Одним из основных этапов проектирования комплексной системы защиты информации является выявление возможных угроз и каналов утечки информации. Также при этом требуется выполнить анализ деятельности предприятия, изучить информационные потоки, проходящие через подразделения, составить перечень конфиденциальной информации, выделить круг лиц, которые имеют доступ к конфиденциальной информации.

Анализ деятельности предприятия. Исследуемое предприятие занимается разработкой концепций построения систем наблюдения за состоянием морских и сухопутных зон, важных в стратегическом и экономическом отношении. Продукция предприятия применяется в пределах морских границ и акваторий, прилегающих к побережью Российской Федерации, а также имеет важное стратегическое и экономическое значение. Предприятие также разрабатывает и изготавливает сухопутные сейсмоакустические средства и системы наблюдения [3].

Функции структурных подразделений предприятия:

- Технический отдел организует решение технических задач и заданий руководства, отвечает за мелкосерийное производство опытных образцов, несет ответственность за выпуск готовой продукции;
- Отдел развития занимается анализом и разработкой перспективных проектов и направлений, оказывает поддержку руководству в процессах анализа и формирования стратегии развития предприятия;
- Служба информационной безопасности регулирует пропускной режим, организует физическую охрану активов, обеспечивает защиту конфиденциальных сведений;
- Отдел экономики и финансов занимается ведением бухгалтерской, финансовой и налоговой отчетности, руководит финансовыми потоками внутренней и внешней среды предприятия;
- Отдел кадров выполняет функции по кадровому обеспечению на предприятии, управлению человеческими ресурсами, ведению личных дел сотрудников;
- Юридический отдел ведет дела, связанные с клиентами предприятия, организует деятельность представителей организации в юридических органах, отвечает за нормативно-правовое обеспечение деятельности организации;
- Производственный отдел выполняет функции по ведению научной деятельности, проведению тестов опытных экземпляров и продукции;
- Серверная лаборатория является основным хранилищем информации предприятия и баз данных.

Анализ информационных ресурсов предприятия. Важным этапом анализа деятельности предприятия является выделение информации, которая представляет ценность. Разглашение такой информации третьим лицам повлечет значительные материальные потери и может проявиться как дестабилизирующий фактор для деятельности и функционирования всего предприятия.

Всю обрабатываемую на предприятии информацию необходимо разделить на общедоступную информацию, доступ к которой неограничен и предоставляется всем без исключения, и информацию, доступ к которой ограничен федеральными законами и регламентом предприятия. В таблице 1 представлен список информационных ресурсов предприятия.

Таблица 1

Список информационных ресурсов предприятия

Информационный ресурс	Общедоступная информация / Информация ограниченного доступа	Сотрудники каких подразделений допущены к информации	В каких помещениях предприятия обрабатывается (хранится) информация	На каких носителях распространяется (хранится) информация
1. Информация в СМИ	Общедоступная	Нет ограничений	Юридический отдел Отдел по развитию	Бумажные Магнитные Оптические
2. Заказы на исследования и разработку (конкурсы и тендеры)	Общедоступная	Нет ограничений	Технический отдел Кабинет ген. директора	Бумажные Магнитные
3. Данные о продажах, финансовое положение предприятия	Общедоступная	Нет ограничений	Бухгалтерский отдел	Бумажные Магнитные Оптические
4. Информация о закупках	Общедоступная	Нет ограничений	Бухгалтерский отдел Производственный отдел Технический отдел	Бумажные Магнитные Оптические
5. Информация о характеристиках продукции	Общедоступная	Нет ограничений	Производственный отдел Отдел информационной безопасности	Бумажные Магнитные
6. Рабочие вакансии предприятия.	Общедоступная	Нет ограничений	Отдел информационной безопасности Отдел кадров	Бумажные Магнитные
7. Запросы на закупку	Ограниченного характера	Юридический отдел Бухгалтерский отдел Производственный отдел Технический отдел	Юридический отдел Бухгалтерский отдел	Бумажные
8. Рабочие документы	Ограниченного характера	Циркулируют между всеми отделами	Циркулируют между всеми отделами	Бумажные
9. Запросы на финансирование	Ограниченного характера	Собрание акционеров Ген. директор Бухгалтерский отдел	Кабинет ген. директора Бухгалтерский отдел	Бумажные Бумажные Магнитные Оптические
	Общедо-	Сотрудники каких	В каких помещениях	На каких

Информационный ресурс	ступная информация / Информация ограниченного доступа	подразделений допущены к информации	предприятия обрабатывается (хранится) информация	носителях распространяется (хранится) информация
10. Приказы и распоряжения	Ограниченного характера	Циркулируют между всеми отделами	Циркулируют между всеми отделами	Бумажные
11. Сведения о конкурентах и их продукции	Ограниченного характера	Производственный отдел Технический отдел Ген. директор Отдел ИБ	Отдел информационной безопасности	Бумажные
12. Данные о продукте, необходимые для производства	Ограниченного характера	Производственный отдел Технический отдел	Производственный отдел Технический отдел	Бумажные Магнитные
13. Сведения о производственных мощностях предприятия	Ограниченного характера	Производственный отдел Технический отдел Ген. директор	Производственный отдел Кабинет ген. директора	Бумажные

На предприятии должен быть сформирован и утвержден перечень сведений, составляющих конфиденциальную информацию предприятия, к которой относится: научно-техническая информация, производственная информация, оперативная (текущая) информация, распорядительные, информационно-справочные и организационные документы предприятия, а также управленческая информация, данные о рынке, информация по безопасности и персональным данным, планы и объемы реализации продукции, сведения о кадровом составе и правилах его формирования.

Построение схемы причинно-следственных связей. Выявление и анализ угроз защищаемой информации является ответственным этапом при построении системы защиты информации на предприятии. Возможные угрозы информационной безопасности предприятия подразделяются на случайные, преднамеренные и естественные. Возможные каналы утечки информации предприятия — это технические, физические, параметрические и каналы, возникающие при внешних атаках и атаках, происходящих внутри корпоративных информационных и коммуникационных систем.

В результате анализа возможных угроз информационной безопасности предприятия и каналов утечки информации формируется схема причинно-следственных связей, так называемая диаграмма Исикавы, которая отражает воздействие различных факторов на информационную безопасность предприятия (рис. 1). Диаграмма позволяет определить главные факторы, оказывающие наиболее сильное влияние на снижение уровня информационной безопасности.

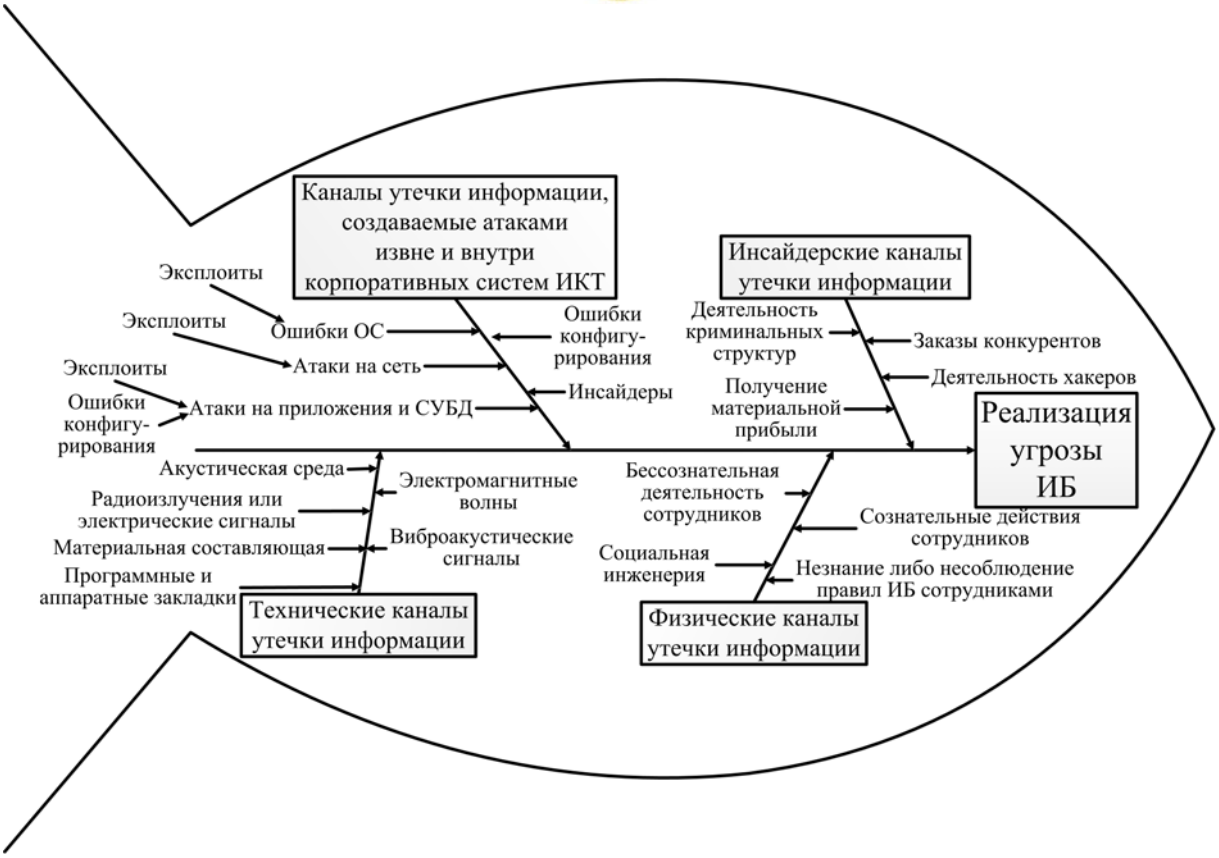
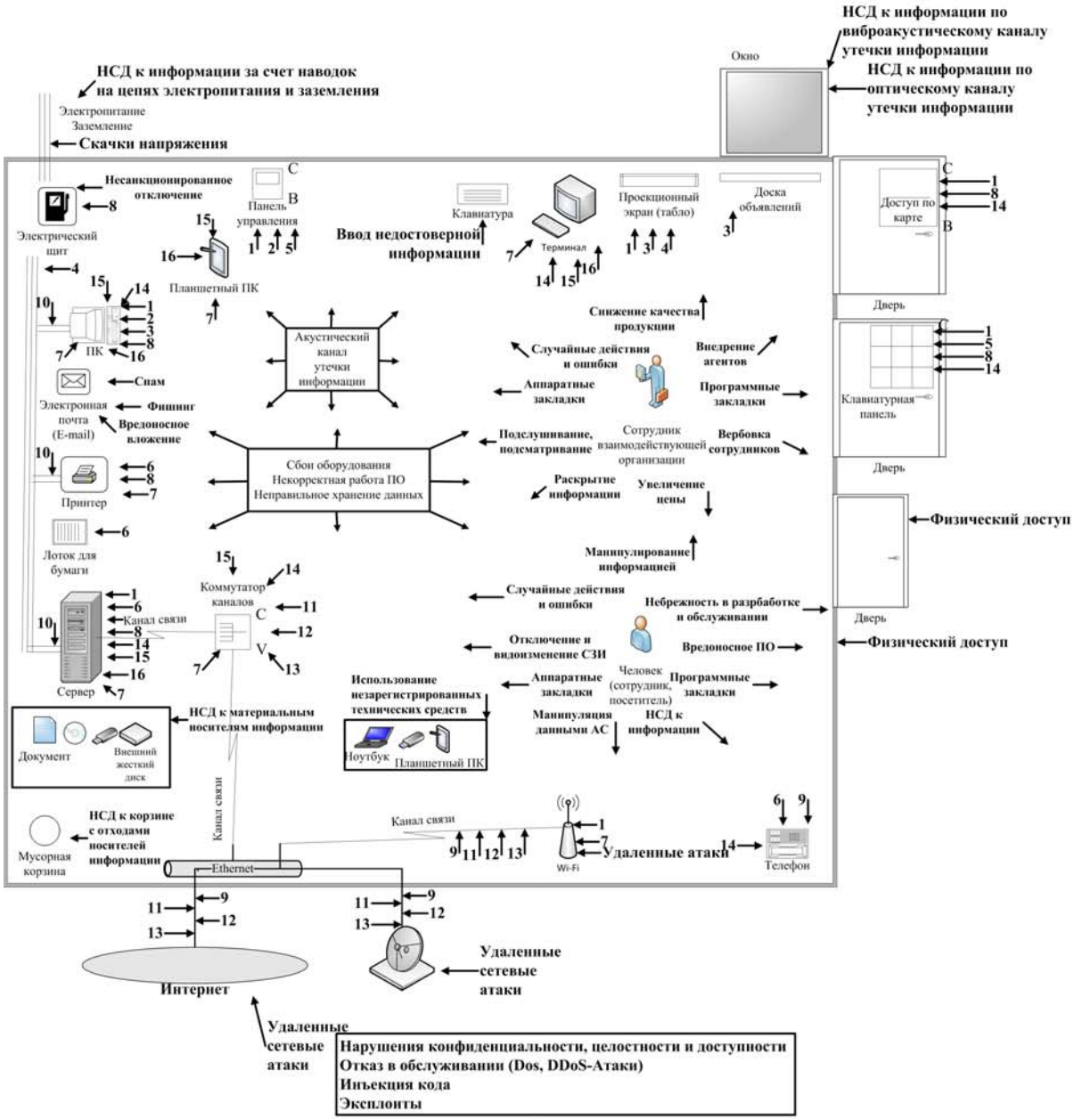


Рис. 1. Схема причинно-следственных связей

С помощью построенной диаграммы Исикавы можно выполнить операции по предупреждению или устранению влияния угроз информационной безопасности, путем введения необходимых технических, программно-аппаратных защитных мер и проведения организационных мероприятий.

Построение модели защиты объекта. Обеспечение безопасности объекта требует учета многих параметров [4–6]. Нередко эту задачу пробуют оперативно решить путем оснащения объекта различными техническими средствами и дорогостоящими специальными системами. Практика показывает, что этот путь не дает ожидаемого результата без четкого понимания угроз, потенциальных нарушителей, особенностей объекта и детальной оценки рисков.

Требуемый уровень безопасности достигается только в том случае, если система защиты представляет собой интегрированный комплекс, объединяющий в себе инженерно-технические средства защиты, организационные меры, регламенты и программные средства сбора, обработки и визуализации данных. Основой для такого подхода служит разработанная модель угроз информационной безопасности объекта защиты (рис. 2).



Внутренние угрозы:

1. НСД к информации при ремонте и техническом обслуживании оборудования
2. НСД к терминалам и ЭВМ
5. НСД к технологическим пультам
6. НСД к носителям информации
8. НСД к внутреннему монтажу аппаратуры
14. Внедрение программных и аппаратных закладок

Внешние угрозы:

Удаленные сетевые атаки

Внутренние / Внешние угрозы:

3. НСД к средствам отображения информации
4. НСД к информации по ПЭМИН
7. НСД к средствам загрузки ПО
9. НСД к линиям и каналам связи
10. НСД к информации за счет наводок на цепях вспомогательной и посторонней аппаратуры
11. НСД к передаваемому трафику
15. Вредоносное программное обеспечение
16. Уязвимости в ПО
12. Внедрение ложного маршрута (MiTM-атака)
13. Незащищенные протоколы передачи и управления

Рис. 2. Модель угроз информационной безопасности объекта защиты

Модель позволяет сформировать и отобразить прямое представление структуры, состава и взаимосвязи составляющих элементов системы защиты информации на предприятии, а также будет способствовать повышению эффективности обеспечения информационной безопасности предприятия.

Заключение (выводы). Проведен анализ угроз и каналов утечки информации предприятия, занимающегося научно-исследовательской и производственной деятельностью. По результатам анализа построены диаграмма Исикавы, отражающая влияние различных факторов на информационную безопасность предприятия, и модель угроз информационной безопасности, описывающая источники возможных угроз информационной безопасности, каналы утечки и компоненты системы защиты информации на предприятии. В ходе работы были проанализированы информационные ресурсы предприятия, сформирован перечень информации ограниченного доступа, проведен анализ информационных потоков предприятия, построены схемы внешних и внутренних информационных потоков предприятия.

Библиографический список.

1. Котляров, В. П. Современный подход к анализу уязвимостей информационных систем // Путь науки. — 2014. — № 9 (9). — Т. 1. — С. 27–28.
2. Партыка, Т. Л. Информационная безопасность / Т. Л. Партыка. — Москва : Форум: ИНФРА-М, 2010. — 368 с.
3. Информация о рынках и компаниях [Электронный ресурс] // РусПрофиль. — Режим доступа : http://www.rusprofile.ru/ (дата обращения: 02.02.2016).
4. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ : [утв. ФСТЭК России от 11 февраля 2013 г. № 17] [Электронный ресурс] // ФСТЭК России. — Режим доступа : http://fstec.ru/normotvorcheskaya/akty/53-prikazy/702/ (дата обращения: 02.02.2016).
5. Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды : приказ : [утв. ФСТЭК России от 14 марта 2014 г. № 31] [Электронный ресурс] // ФСТЭК России. — Режим доступа : http://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (дата обращения: 02.02.2016).
6. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ : [утв. ФСТЭК России от 18 февраля 2013 г. № 21]. [Электронный ресурс] // ФСТЭК России. — Режим доступа : http://fstec.ru/normotvorcheskaya/akty/53-prikazy/691 (дата обращения: 02.02.2016).