УДК 620.9

АНАЛИЗ ОСОБЕННОСТЕЙ РАЗРАБОТКИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРОМЫШЛЕННОМ ПРЕДПРИЯТИИ

© 2023 Т. В. Аветисян[1, 2], А. П. Преображенский[2]

[1]Колледж Воронежский институт высоких технологий (Воронеж, Россия)
[2]Воронежский институт высоких технологий (Воронеж, Россия)

В статье дается анализ особенностей разработки системы защиты информации на промышленном предприятии. Выделяются соответствующие уровни, на которых проводится защита информации. Приведена классификация информации, которая циркулирует внутри производственной системы. Показано, каким образом можно определить стоимость информации.

Ключевые слова: предприятие, защита информации, управление, процесс.

В данной статье мы будем проводить анализ подходов и систем, связанных с защитой информации (СЗИ) на промышленном предприятии. Кроме того, рассматриваются методы, направленные на разработку эффективной системы, позволяющей осуществлять информационную безопасность.

Для первого этапа разработки СЗИ важно определиться со степенью защищенности промышленного предприятия. Это связано с тем, на сколько конфиденциальными будут данные, которые есть на предприятии, и главное, какой может возникнуть ущерб, если произойдет их утечка.

Тогда, цель защиты организации может быть сформирована таким образом: обеспечение защищенности промышленного предприятия от угроз, связанных с нарушением информационной безопасности, а также сохранением конкурентоспособности. В нее входят показатели, которые относятся к конфиденциальности, целостности, а также доступности информации.

После постановки цели происходит переход от комплексного поэтапного процесса формирования систем защиты информации к стадии, в которой поддерживается работоспособность созданного рабочего варианта СЗИ.

Кроме того, если создается СЗИ важно обращать внимание на то, что уровень должен быть достаточным. Это связано с тем, что злоумышленники достаточно часто замечают, что кроме больших и средних предприятий, малые в меньшей степени заинтересованы в том, чтобы обеспечивать информационную безопасность (ИБ).

В результате, злоумышленникам проще осуществлять кражи данных из нескольких небольших предприятий, чтобы остаться незамеченным. При этом применяются специальные программы, которые проводят сканирование незащищенных устройства, осуществляя передачу данных заинтересованным людям [1].

Можно сделать вывод, что все предприятия должны уделять соответствующее внимание ИБ [2], если обрабатывается новая информации. Тогда необходимо использовать различные базы данных [3], чтобы предприятия были обладателями конкурентных преимуществ.

Если решаются задачи, связанные с защитой информации, которая содержится внутри информационно-телекоммуникационных систем, то реализуется принятие решения относительно необходимости формирования СЗИ сетевых структур, а еще определяются цели и задачи защиты информации внутри сетевых структур [4].

Внутри различных систем защиты информации есть возможности для определения объектов, относительно которых необходимо обеспечивать защиту. СЗИ рассматривается в виде множества органов и исполнителей, которые применяют технику защиты информации.

Аветисян Татьяна Владимировна – Колледж Воронежского института высоких технологий; Воронежский институт высоких технологи, преподаватель, e-mail: vtatyana_avetisyan@mail.ru.
Преображенский Андрей Петрович – Воронежский институт высоких технологий, доктор техн. наук, профессор, e-mail: app@vivt.ru.

Существуют также объекты защиты информации. Это множество организуется и функционирует в рамках правил и норм, которые устанавливаются на базе соответствующих документов в сфере защиты информации [5]. Реализация организационных и технических мер защиты информации, происходит на основе СЗИ, которые обрабатывают тот объем информации, который относится к информационно-телекоммуникационной системе [6].

Подобно персональным данным [7], можно выделить соответствующий тип конфиденциальной информации, связанный с коммерческой тайной.

Проведя анализ, можно сказать, что необходимо обеспечивать защиту любой информации, неправомерная работа с которой может привести к ущербу ее обладателям [8]. Помимо этого, проведение защиты информации можно рассматривать в виде обязанности, а не только в виде права.

Большей частью, с данными, связанными с государственной тайной, не будут работать промышленные предприятия, внутри которых не сформирован соответствующий режим, определяемый Законодательством РФ.

Если обнаруживается утечка данных, то она может отрицательным образом оказывать влияние на функционировании предприятий. Но составить универсальный список для данных, требующих защиты, не всегда просто.

С другой стороны, основываясь на целях и задачах в бизнес-процессах конкретного промышленного предприятия происходит формирование перечня сведений, которые необходимо защищать. Среди анализируемых данных мы можем указать следующие:

- персональные данные по сотрудникам и клиентам;

- составляющие финансовых документов;

- договоры и контракты, которые уже заключены, и существуют в ходе разработок. Для незавершенных сделок необходима поддержка по защите в большей мере. Это связано с тем, что конкуренты после совершения анализа по предложенным условиям, могут провести формулирование более выгодного предложения. Тогда они смогут выиграть в ходе конкурентной борьбы;

- информация, связанная с товарами и услугами, которые будут предоставляться промышленным предприятием;

- данные, связанные с поставщиками;

- характеристики состояния материальных запасов, резервов.

В ходе формирования подобного списка мы можем использовать технологическую помощь со стороны внешних аудиторов. Еще есть способ, позволяющий создавать комиссию из специалистов, которые будут составлять перечень данных, для которых важно обеспечивать защиту.

После того, как данные, подлежащие защите, обозначены, для них следует обозначить уровень доступности.

Когда ведется градационное деление информации, тогда в качестве критерия может рассматриваться величина денежной оценки по возможным ущербам. Ее мы можем достичь на базе метода экспертных оценок. Основная его идея связана с тем, что ведется опрос по группе экспертов. В качестве экспертов могут рассматриваться специалисты, помогающие в составлении предварительного списка данных, для которых требуется поддержка по защите.

На рисунке дана классификация информации.

Мы можем ранжировать выделенные данные относительно стоимости информационных ресурсов, если предприятие является негосударственным.

По открытым каналам внутри информационных потоков предприятий свободным образом проходит общедоступная информация.

На основе сформированной экспертной комиссии из специалистов осуществляется оценка по различным видам информации при учете ключевых видов угроз нарушений.

После этого необходимо провести исследование, связанное с определением стоимости информации. При этом разработчики могут опираться на стандарт ИБ ISO 27001.

Значение стоимости информации (СИ) может быть определено в виде суммы таких элементов (1).

$$СИ = РС + ВП + НП; \quad (1)$$

В указанном выражении РС – значение рыночной стоимости информации; ВП – значения возможных дополнительных потерь; а НП – значение недополученной

прибыли. Надо признать, что проведение оценки по всем слагаемых является задачей весьма трудоемкой. В этой связи значения оценок могут быть достаточно приблизительными.

Рисунок. Классификация информации, которая циркулирует в производственной системе

Если будет нарушаться конфиденциальность информации при оценках стоимости информационных ресурсов мы можем наблюдать: уменьшение контрактов; ущерб, связанный с раскрытием конфиденциальных сведений; потерю клиентов; затраты на восстановление связей с клиентами и поставщиками; осуществление снижения по стоимости акций предприятия; затраты на восстановление положительного имиджа предприятия.

В случае нарушения целостности информации при оценках стоимости ресурсов рекомендуется учитывать такие параметры: время, связанное с повторным вводом потерянной информации, время, связанное с восстановлением целостности ресурсов.

Если нарушается доступность информации, то ведется оценка времени простоя и упущенной выгоды.

После того, как пройден этап оценок стоимости каждого из информационных ресурсов, которые должны быть защищены, важно осуществить процесс ранжирования по классам. Он ведется исходя из того, какая стоимостная величина: низкая, средняя, высокая. Каждое предприятие делает отбор наименования классов и диапазонов совокупной стоимости самостоятельным способом.

Если все отмеченные этапы осуществлены как приказ по предприятию, то происходит публикация документа «Перечень сведений, подлежащих защите». После этого мы можем переходить к анализу рисков.

Вывод. Процессы защиты информации на предприятии должны рассматриваться в виде совокупности нескольких этапов. Для каждого этапа требуется формирование целей и списка задач. Они решаются на базе обозначенных критериев.

СПИСОК ИСТОЧНИКОВ

1. Львович И. Я. Применение методологического анализа в исследовании безопасности / И. Я. Львович, А. А. Воронов // Информация и безопасность. – 2011. – Т. 14. – № 3. – С. 469-470.

2. Преображенский Ю. П. Информационная безопасность – вызовы современного мира / Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2017. – № 2 (21). – С. 60-63.

3. Преображенский Ю. П. Об обеспечении безопасности корпоративной сети / Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2018. – № 2 (25). – С. 47-50.

4. Львович Я. Е. Особенности оптимизации беспроводных систем связи / Я. Е. Львович, Ю. П. Преображенский, Е. Ружицкий // Вестник Воронежского института высоких технологий. – 2022. – № 1 (40). – С. 68-71.

5. Львович Я. Е. Многометодный подход к моделированию сложных систем на основе анализа мониторинговой информации / Я. Е. Львович, А. В. Питолин, Г. П. Сапожников // Моделирование, оптимизация и информационные технологии. – 2019. – Т. 7. – № 2 (25). – С. 301-310.

6. Родионова В. О. Исследование и моделирование организационной культуры региональных конкурентоспособных машиностроительных предприятий / В. О. Родионова, Н. В. Федоркова // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. – № 3 (38). – С. 7-8.

7. Коровин Е. Н. Применение методики "Servqual" с проведением HR-бенчмаркинга для оценки удовлетворенности персонала организации / Е. Н. Коровин, М. В. Кривоносова // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. – № 3 (38). – С. 1-2.

8. Акулова А. Д. Разработка матрицы для Swot-анализа на основе ключевых параметров и критериев, учитывающих особенности управления медицинской организацией / А. Д. Акулова, Е. Н. Коровин // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. – № 3 (38). – С. 5-6.

9. Львович И. Я. Моделирование процесса управления промышленными организациями на основе рейтингового подхода / И. Я. Львович [и др.] // Моделирование, оптимизация и информационные технологии. – 2020. – Т. 8. № 3 – (30). – Доступно по: https://moitvivt.ru/ru/journal/article?id=834 (дата обращения 10.09.2022).

THE ANALYSIS OF THE FEATURES OF THE DEVELOPMENT OF AN INFORMATION SECURITY SYSTEM IN AN INDUSTRIAL ENTERPRISE

© 2023 T. V. Avetisyan[1, 2], A. P. Preobrazhenskiy[2]

[1, 2]College Voronezh Institute of High Technologies (Voronezh, Russia)
[2]Voronezh Institute of High Technologies (Voronezh, Russia)

The paper analyzes the features of the development of an information security system at an industrial enterprise. The appropriate levels at which protection is carried out are allocated. An illustration of how the information that circulates within the production system is classified. It is shown how to determine the cost of information.

Keywords: enterprise, information protection, management, process.