УДК 004.777

СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Габрусь Е.В.

гр.367241

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Борботько Т.В. – доктор технических наук, заведующий кафедрой защиты информации, профессор

Аннотация. В материалах доклада рассматривается разработка полномасштабной системы управления информационной безопасностью, которая выполняет функции комплексного управления, мониторинга и аудита информационной безопасности. Представлена система управления информационной безопасностью, основанная на принципах конфигурационного управления.

Ключевые слова: управление, архитектура системы

Введение. В настоящее время практически ни одна организация не обходится без использования IT-технологий. Данные, обрабатываемые в информационных системах, могут иметь высокую ценность для компании. В таких случаях становится неприемлемым нарушение тех или иных характеристик безопасности (конфиденциальности, целостности и доступности) критичной информации, поскольку это может привести не только к серьезному ущербу, но и поставить под сомнение дальнейшее существование организации. В связи
с этим появляется необходимость в обеспечении защиты информации, обрабатываемой компанией.

Безусловно, необходимо использовать комплексный подход, содержащий в себе как применение организационных мер, так и использование технических (в том числе программных и аппаратно-программных) средств защиты информации.

Основная часть. Основным способом обеспечения непрерывной деятельности предприятия является организация отказоустойчивости бизнес-процессов, производственных процессов, экономической и управленческой сферы. Однако в связи с ростом автоматизации задач, решаемых в рамках деятельности предприятия, остро стоит вопрос об обеспечении сохранности конфиденциальной информации, коммерческой и государственной тайны.
На ряду с применением специализированных средств противодействия кражи информационных ресурсов (далее – ИР) могут быть использованы система управления информационной безопасностью (далее – СУИБ) или система мониторинга защищённости информации (далее – СМИ). Ежегодно данные отчётов ведущих компаний об утечках информации и их последствиях: частичное или полное приостановление деятельности предприятий, огромные финансовые потери, говорят о необходимости не только обеспечения информационной безопасности (далее – ИБ), восстановлении информации после сбоя работы систем, но и об обеспечении комплексного управления ИБ.

Таким образом средняя утечка данных (количество данных на один случай) составила 2,93 миллиона записей, что на 35,2% меньше, чем в 2021 году (4,52 миллиона записей). Скорее всего, реальный «вес» одной утечки оказался выше, так как доля случаев, когда количество утекших записей была неизвестной, в 2022 году составила 58,8%. Однако, в 2021 году доля таких инцидентов была еще выше – 63,2%. Резкий рост количества утечек данных в последние годы главным образом

был спровоцирован беспрецедентным увеличением активности внешних злоумышленников, в том числе гибридных атак. Отчет компании InfoWatch по распределению утечек информации в мире по вектору воздействия за период 2017-2022 годы, с учетом неопределенных (то есть когда источник утечки определить не представляется возможным), приведен на рисунке 1.

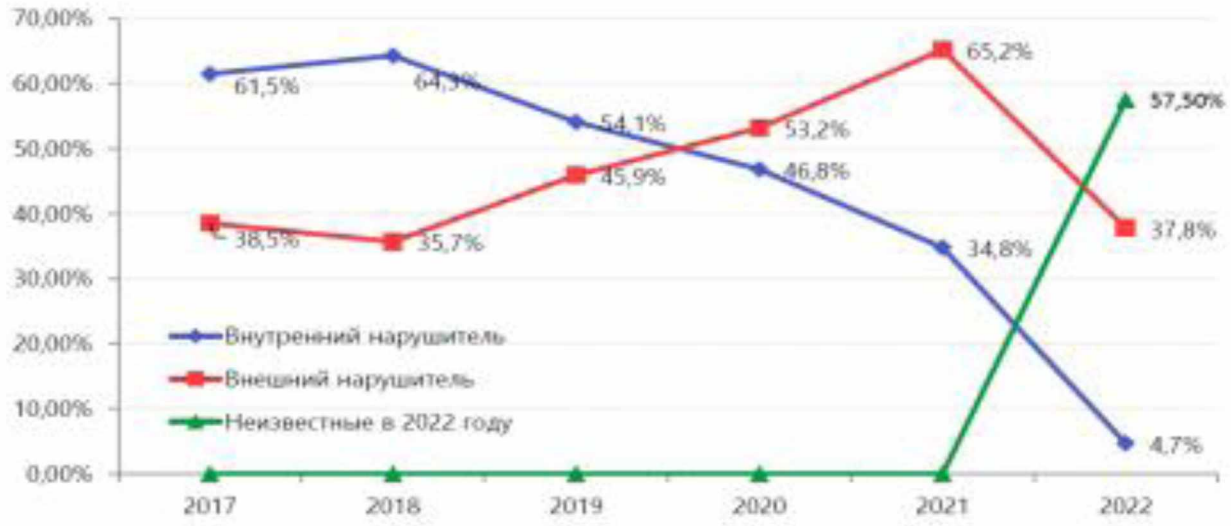

Рис 3. Распределение утечек информации по вектору воздействия (внешний/внутренний),%: Мир, 2017–2022 гг.

Рисунок 1 – Результаты исследования утечек информации компанией InfoWatch

Можно сделать вывод, что, не смотря на усовершенствование методик по защите информации, улучшение качества систем защиты информации (далее – СЗИ), хакерские навыки по осуществлению взлома СЗИ и выводу из строя защищаемых информационных систем позволяют достигнуть им своей цели: хищения критически важных ИР. При высокой численности утечек конфиденциальной информации, последствия для предприятий критические: невозможность найти виновного в краже информации, финансовые потери, рост социальной инженерии. По данным Zecurion Analytics за 2014 год, максимальный ущерб от одного инцидента ИБ в российских компаниях составил 30 миллионов долларов, средний ущерб в мире от одной утечки– 25 миллионов долларов. Из информации, представленной выше, следует, что кражи и утечки ИР увеличиваются, а убытки, нанесенные предприятиям, растут. Анализ показал, что применение СУИБ и СМИ позволяет снизить риски нарушения ИБ и оказать противодействие несанкционированному доступу к информации. Однако часто сложная реализация таких систем приводит к трудностям, возникающим при внедрении и использовании механизмов управления. Таким образом, СУИБ и СМИ должны обладать гибким механизмом администрирования. Современные СУИБ решают специализированную задачу, а не совокупность задач, это не позволяет использовать технологию комплексного управления. Для проектирования и реализации СУИБ предприятия, специалистами используется определенный метод управления: кибернетический (основан на принципах кибернетики и модели «черного ящика»), организационный (утвержденная политика ИБ и система внутренних документов, регламентирующих основные положения ИБ), процессный подход (непрерывность функционирования управленческих процессов), оптимизационный (поиск и применение оптимальных функций управления). Для

достижения эффективного управления ИБ, необходимо применять комплексный подход, представляющий собой совокупность методов управления, описанных выше. В качестве исследуемой проблемы предложена СУИБ, архитектура которой представлена на рисунке 2.

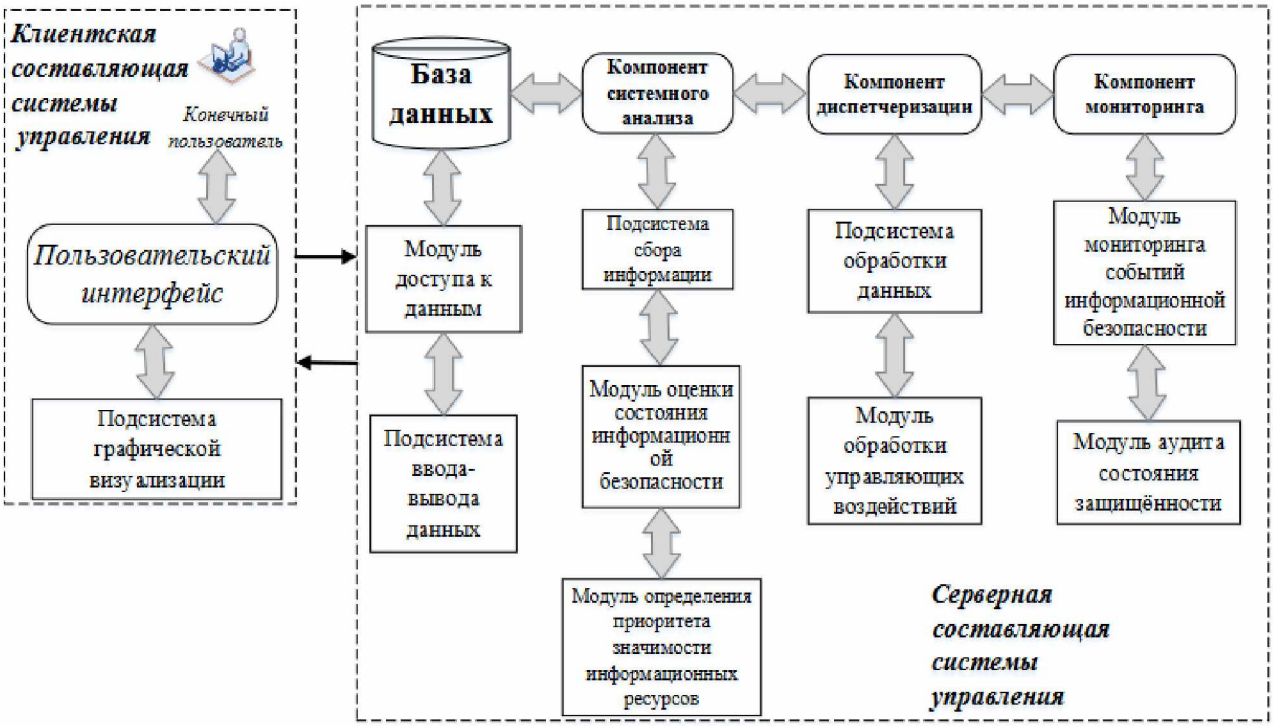

Рисунок 2 – Архитектура системы управления информационной безопасностью предприятия

Так как СЗИ распределенные и многозадачные, при разработке СУИБ будет использоваться концепция конфигурационного управления. Запланированная к разработке СУИБ представляет собой клиент-серверную систему. Клиентская часть позволяет взаимодействовать пользователю (специалисту по ИБ) с СУИБ по средствам пользовательского интерфейса. Для наглядного отображения функций управления в СУИБ заложена подсистема графической визуализации. Серверная часть включает в себя базу данных, компонент системного анализа, компонент диспетчеризации и компонент мониторинга. СУИБ объединяет функционирование четырех подсистем и шести модулей. Отличие запланированной к разработке СУИБ от ранее предложенных заключается в том, что набор конфигураций, позволяет сформировать систему многоуровневого управления.

Заключение. Таким образом разработка и внедрения СУИБ и информационных технологий неразрывно связаны со стандартизацией процессов их управления, созданием нормативной, методической и регламентирующей базы. Кроме того, СУИБ отвечает за планирование, исполнение, контроль и техническое обслуживание всей инфраструктуры безопасности. Эффективность системы ИБ и труда администраторов средств ИБ будет чрезвычайно низкой при отсутствии средств сбора, анализа, хранения информации о состоянии системы ИБ, централизованного управления всеми ее составляющими. Дело в том, что каждое средство защиты реализует некоторую составляющую политики безопасности, которая на уровне подсистем задается набором параметров и требований.

Список литературы

1. Панасенко А.А. Конфиденциальные данные продолжают утекать. [Электронный ресурс]. – Режим доступа: http://www.anti-malware.ru/analytics/Threats_Analysis/Sensitive_data_continue_leak – Дата доступа: 15.02.2024.

2. Zecurion Analytics. Утечки конфиденциальной информации [Электронный ресурс]. – Режим доступа: http://www.zecurion.ru/upload/iblock/fe3/Zecurion_Data_leaks_2015.pdf – Дата доступа: 15.02.2024.

3. Сердюк Н.Н. Архитектура информационно-аналитической системы управления безопасностью производства. / Н.Н. Сердюк // Автоматизированные системы управления и приборы, 2014, № 167.

4. Козунова С.С. Информационная система управления информационной безопасностью организации // Наука и Мир. 2016. Т. 1. № 4(32), 59-60 с.

5. Козунова С.С., Бабенко А.А. Автоматизация управления инвестициями в информационную безопасность предприятия //Вестник компьютерных и информационных технологий, 2015, № 3 (129), 38-44 с.

UDC 004.777

INFORMATION SYSTEMS SECURITY MANAGEMENT SYSTEM

Habrus Y.V.

gr.367241

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Borbotko T.V. – Dr. of Sci. (Tech.), head of the department of information security, *professor*

Annotation. The report discusses the development of a full-scale information security management system, which performs the functions of integrated management, monitoring and audit of information security. An information security management system based on the principles of configuration management is presented.

Keywords: management, system architecture