УДК 004.056.5
DOI 10.33764/2618-981X-2022-6-122-126

Комплексная защита информации на производственном предприятии

Е. Э. Кулеш[1]*, *Р. А. Смирнов*[1], *Г. В. Попков*[1]
[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: tastaeva.k@yandex.ru

Аннотация. Разработка комплексной системы защиты информации отражает системный подход к обеспечению информационной безопасности предприятия, предотвращению хищений и утечек информации ограниченного доступа, а также оптимизирует работу ИТ-системы предприятия, сокращает капитальные и операционные расходы организации. Обеспечение информационной безопасности на производстве имеет свои «тонкости», связанные с особенностью автоматизированных систем управления предприятием и со спецификой хода производственных процессов. Настройка системы информационной безопасности потребует высокого внимания, так как любая ошибка может привести не только к сбою, но и к аварии. В результате исследования комплексной защиты информации на производственном предприятии были получены следующие результаты: определены особенности информационной безопасности на предприятии, проведен анализ актуальных угроз безопасности, рассмотрены вопросы реализации системы защиты информации на предприятии.

Ключевые слова: информационная безопасность, комплексная защита информации, автоматизированная система управления

Comprehensive Information Protection at the Manufacturing Plant

E. E. Kulesh[1]*, *R. A. Smirnov*[1], *G. V. Popkov*[1]
[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: tastaeva.k@yandex.ru

Abstract. The development of an integrated information security system (hereinafter referred to as KSI) reflects a systematic approach to ensuring information security (hereinafter referred to as IS) of the enterprise, preventing theft and leaks of restricted access information, and also optimizes the operation of the enterprise's IT system, reduces capital and operating expenses of the organization. Ensuring information security in production has its own "subtleties" associated with the peculiarity of automated control systems (hereinafter - ACS) of the enterprise and with the specifics of the course of production processes. Setting up an information security system will require high attention, since any error can lead not only to failure, but also to an accident. As a result of the study of complex information protection at a manufacturing enterprise, the following results were obtained: the features of information security at the enterprise were determined, the analysis of current security threats was carried out, the issues of implementing an information protection system at the enterprise were considered.

Keywords: information security, comprehensive information protection, automated control system

Актуальность и проблема комплексной защиты информации

В настоящее время очень актуальна тема защиты информации на предприятии, так как глобальный рынок защиты информации предлагает множество отдельных инженерно-технических, программно-аппаратных криптографической

средств защиты информации. Чтобы создать условия для эффективной защиты информации на предприятии, необходимо объединить отдельные средства защиты в единую систему.

Разработка комплексной защиты информации – главная задача любого предприятия – это и является главной проблемой производственных предприятий. При этом создаваемый комплекс защиты информации не должен приводить к ощутимым трудностям в работе предприятия, а разработка комплекса защиты информации должна быть экономически обоснованной.

Основными составляющими комплексной системы защиты информации являются организационное обеспечение информационной безопасности, а также программно–аппаратные средства, исключающие несанкционированный доступ к защищаемой информации [3].

Целью данной работы является исследование наиболее актуальных угроз безопасности информации на производственном предприятии, а также способы защиты от этих угроз.

Для достижения цели необходимо решить ряд задач:

– рассмотреть особенности информационной безопасности на предприятии;

– провести анализ актуальных угроз безопасности на производственном предприятии;

– рассмотреть вопрос реализации системы защиты информации на производстве;

– рассмотреть особенности обеспечения комплексной защиты информации на объектах критическая информационная инфраструктура (КИИ).

Особенности информационной безопасности на предприятии

Понятие «информационная безопасность» предполагает обеспечение доступности, целостности, конфиденциальности информации. Основными особенностями информационной безопасности в производстве являются [1]: помимо рабочих станций и элементов инфраструктуры, производственные единицы становятся объектами управления. Это могут быть станки с ЧПУ, системы жизнеобеспечения электростанции и т.д. Часто они не статичны, а находятся в движении.

Особенности промышленных информационных сетей также порождают особенности направленных на них угроз информационной безопасности.

Анализ актуальных угроз безопасности на производственном предприятии

Большое количество сетевых соединений упрощает управление удаленными и движущимися объектами, но создаёт дополнительные угрозы. Одна из крупнейших производственных компаний в мире – «Siemens», предложила актуальную классификацию угроз безопасности информации [7]:

– несанкционированное использование удаленного доступа к процессу управления производственным объектом. Каналы связи Автоматизированной системы управления (АСУ) обычно не имеют достаточной защиты;

– хакерские атаки, направленные через корпоративные (офисные) информационные сети. Имеются связи между каналами управления АСУ и офисной информационной системой, которые могут использоваться злоумышленниками;

– атаки на стандартные компоненты инфраструктуры сетей управления АСУ. Информационные системы имеют уязвимости, которые не всегда своевременно устраняются разработчиками, но хорошо известны злоумышленникам. При наличии таких компонентов в архитектуре АСУ они могут использоваться для атаки;

– DDoS-атаки. Атаки типа «отказ в обслуживании» часто используются для нарушения сетевых соединений и нормальной работы АСУ;

– ошибки персонала, преднамеренные диверсии и повреждения элементов системы управления;

– внедрение вирусных и других вредоносных программ через съемные носители лицами, допущенными к обслуживанию оборудования.

Реализация системы защиты информации на производстве и методика исследования

Система безопасности, реализованная для АСУ, должна отвечать требованиям ГОСТ Р МЭК 62443-2-1-2015 [2], являющегося основным стандартом безопасности в системах промышленной автоматизации.

Решение проблемы комплексной системы защиты информации от атак:

– физических атак;

– несанкционированного доступа сотрудников и третьих лиц;

– хакерских атак.

При разработке собственной системы организации информационной безопасности на производстве следует учитывать, что успех ее развертывания зависит от следующих факторов:

– необходимость мониторинга коммуникационных интерфейсов между офисными и промышленными сетями, каналов удаленного доступа к услугам через Интернет, обеспечения установки межсетевых экранов;

– создания демилитаризованных зон (DMZ), предназначенных для обмена информацией со смежными сетями и исключающих получение внешними пользователями прямого доступа к АСУ;

– создания безопасных сегментов сети для отдельных защищенных производственных секторов, что позволяет снизить риски и увеличить уровень информационной безопасности;

– использования при передаче данных протоколов VPN и шифрования;

– защиты коммуникационных станций алгоритмами аутентификации.

Реализация данных компонентов необходима в любой промышленной системе.

Особенности комплексной защиты информации на объектах КИИ

На сегодняшний день обеспечение комплексной защиты информации на объектах КИИ является важным аспектом в информационной безопасности.

Безопасность КИИ – это комплексный процесс по обеспечению устойчивого и бесперебойного функционирования критичных бизнес– процессов предприятия [9]. Данный процесс включает в себя мероприятия по защите информа-

ции в информационных системах, автоматизированных системах управления технологическими процессами (АСУ) и информационно-телекоммуникационных сетях, которые решают следующие задачи:

– оценка текущего состояния защищённости информационной инфраструктуры предприятия;

– категорирование объектов КИИ;

– разработка и внедрение комплексных систем защиты информации для значимых объектов КИИ предприятия;

– сопровождение и эксплуатация программно-аппаратных средств защиты информации объектов КИИ;

– обеспечение безопасности значимого объекта КИИ при выводе его из эксплуатации.

Создавая комплексную систему защиты информации значимых объектов КИИ, сводятся к минимуму риски остановки производства из-за компьютерных инцидентов, что может негативно повлиять на деятельность предприятия, а если нарушение работы привело к чрезвычайной ситуации, влияющей на безопасность сотрудников, то к уголовной ответственности.

Требования по обеспечению комплексной защиты информации необходимо выполнять субъектам КИИ, которыми согласно ФЗ №187 являются государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, АСУ, функционирующие на производственном предприятии.

Заключение

В результате, можно сделать вывод, какие исследования комплексной защиты информации на производственном предприятии были получены: определены особенности информационной безопасности на предприятии, проведен анализ актуальных угроз безопасности, рассмотрены вопросы реализации системы защиты информации на предприятии. Чтобы не допускать угрозы и риски на производственном предприятии, нужно своевременно проводить анализ, решать вопросы о защите информации предприятия, индивидуально и тщательно подбирать комплекс по защите информации.

В связи с этим, можно сделать вывод о том, что комплексная защита информации должна создаваться и обеспечиваться на каждом производственном предприятии, причем это должно производиться индивидуально для каждого производственного предприятия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту информации объектов информатизации. – учебное пособие. – СПб: НИУ ИТМО, 2011. – 112 с.

2. ГОСТ Р МЭК 62443-2-1-2015 Национальный стандарт Российской Федерации. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы – Москва URL: https://docs.cntd.ru/document/1200121982 (дата обращения: 10.04.2022) – Текст:

электронный. - Режим доступа: для авторизир. пользователей. Баданин // Наука –Информационная Безопасность: сб. науч. тр. – Новосибирск, 2022. – Вып. 62. - С. 8-12.

4. Дудкина, И. А. Технологии и методы обеспечения комплексной защиты информации // Молодой ученый. – 2016. – № 16 (120). – С. 37-39.

5. Безопасность промышленных информационных систем – Россия, Москва. URL: https://cyberleninka.ru/article/n/bezopasnost-promyshlennyh-informatsionnyh-sistem-vidy-ugroz-i-obschie-printsipy-zaschity-informatsii (дата обращения: 11.04.2022) – Текст: электронный. - Режим доступа: для авторизир. пользователей.

7. Комплексная защита информации. – Россия, Санкт-Петербург - URL: https://www.gaz-is.ru/reshenija/resheniya/kszi.html (дата обращения: 15.04.2022) Текст: электронный. – Режим доступа: для авторизир. пользователей.

8. Компания «Siemens Russia». – Россия URL: https://new.siemens.com/ru/ru/kompaniya/o-nas.html (дата обращения: 18.04.2022) – Текст: электронный. – Режим доступа: для авторизир. пользователей.

9. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ – Москва, Россия URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 18.04.2022) - Текст: электронный. - Режим доступа: для авторизир. пользователей.