10. Dyadkin I., Hamilton K. A study of 128–bit multipliers for congruential pseudorandom number generators // REF. IN COMP. PHYS. COMMUN. 125, 2000.

11. Dyadkin I., Hamilton K. A study of 64–bit multipliers for pseudorandom number generators // Computer Physics Communications. 103, 1997. – Pp. 103–130

12. Sezgin, F. A random number generator for 16–bit microcomputers // Computers and Operations Research. Vol. 23, No. 2, 1996. – Pp. 193–198.

13. Borosh I., Niederreiter H. Optimal multipliers for pseudo–random number generation by the linear congruential method // BIT 23, 1983. – Pp. 65–74.

14. Fishman G., Moore L. An exhaustive analysis of multiplicative congruential random number generators with modulus 2^{31} // SIAM Journal on Scientic and Statistical Computing 7, no. 1, 1986 – Pp. 24–45.

15. Fishman G. Multiplicative congruential random number generators with modulus 2^{β}. An exhaustive analysis for 2^{32} and a partial analysis for 2^{48} // Mathematics of Computation 54, no. 189, 1990. – Pp. 331–344.

16. L'Ecuyer P., Couture R. An implementation of the lattice and spectral tests for multiple recursive linear random number generators // INF ORMS Journal on Computing 9, no. 2, 1997. – Pp. 206–217.

17. Бараш Л.Ю., Щур Л.Н. Генерация случайных чисел и параллельных потоков случайных чисел для расчетов Монте–Карло // Моделирование и анализ информационных систем. 2012; 19(2). – С. 145–162.

18. Matsumoto M., Nishimura T. Dynamic Creation of Pseudorandom Number Generators // Monte Carlo and Quasi–Monte Carlo Methods, Springer, 2000. – Pp 56–69.

19. Измерение времени работы фрагментов программ: метод. указания / сост. К.Е. Климентьев. – Самара: Изд–во Самар. ун–та, 2018.

С.С. Козунова

УПРАВЛЕНИЕ РИСКАМИ БЕЗОПАСНОСТИ В ПРОМЫШЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

(АО «ФНПЦ «Титан-Баррикады)

За последнее десятилетие текущая ситуация в отечественной промышленности позволяет отметить, что в Российской Федерации рынок производственно-технологического оборудования и промышленных информационных систем успешно сформировался. В промышленной отрасли и различных промышленных видах деятельности образовываются и активно развиваются новые более крупные министерства, корпорации, федеральные органы исполнительной власти, объединённые заводы и консорциумы: Государственная корпорация по космической деятельности «Роскосмос», Министерство промышленности и торговли Российской Федерации, Государственная корпорация «Ростех», АО «Корпорация «СПУ – ЦКБ ТМ», ПАО «Корпорация «Иркут», и другие,

объединяющие под своим началом предприятия, задействованных в сферах проектирования и производства промышленной продукции.

Для автоматизации промышленных предприятий (ПП) и различных отраслей промышленности, для оптимизации бизнес-процессов ПП внедряют специальные информационные системы (ИС) [1, 2]. Промышленные ИС обеспечивают автоматизацию производственных и технологических процессов, цифровизацию проектирования выпускаемой продукции, оптимизацию и реинжиниринг бизнес-процессов (БП), организацию работы электронного документооборота, мониторинг функционирования технологического оборудования [2, 3].

Особенности таких систем, их назначения, сложное строение и архитектура, техническое, программное и информационное обеспечения корпоративных информационных сетей ПП, а также динамическое развитие угроз и дестабилизирующих факторов промышленных ИС [4, 5] подвергают промышленные системы высокому числу рисков и обуславливают необходимость непрерывного мониторинга и контроля текущего уровня рисков безопасности с дальнейшей генерацией и применением решений, направленных на снижение уровня рисков и повышения эффективности управления рисками.

Архитектура промышленных ИС изображена на рисунке 1. Отметим, что промышленные ИС функционируют в корпоративной информационной сети предприятия. Одним из важных аспектов при управлении рисками является анализ информационно-сетевых потоков [3, 6]. Компонентами промышленных ИС являются блоки: административные здания (например, удалённые филиалы или здания), центр обработки данных (ЦОД), производственный уровень.

Производственный уровень и/или ЦОД функционируют в промышленных сетях, которые являются подсетями корпоративной информационной сети или обособленной сетью. Эти подсети отделены межсетевым экранированием или VLAN (построением виртуализации). Административное здание предприятия представляет собой объект, в котором сосредоточены серверные помещения, автоматизированные рабочие места, устройства и сотрудники. ЦОД предназначен для размещения и использования вычислительного оборудования. Он позволяет обрабатывать данные и выступает в качестве дата-центра.

На производственном уровне исследуемых систем функционируют технологические линии, комплексы, датчики и иное специальное производственное оборудование (станки, производственные агрегаты, печи, прессы).

В настоящее время на промышленных предприятиях тематика обеспечения информационной безопасности (ИБ) приобретает всё более высокую актуальность [5, 7]. Несмотря на наличие многочисленных исследований области управления рисками промышленных ИС, проблемы оценки и управления рисками таких систем затрагивались частично. До сих пор отсутствует комплексная методика управления рисками ИБ в промышленных ИС. Научные работы, в которых рассматривались проблемы обеспечения ИБ промышленных ИС, затронули только общие проблемы без конкретизации. Результаты научных ис-

следований в данной области часто являются информацией, составляющей коммерческую тайну современных крупномасштабных предприятий.

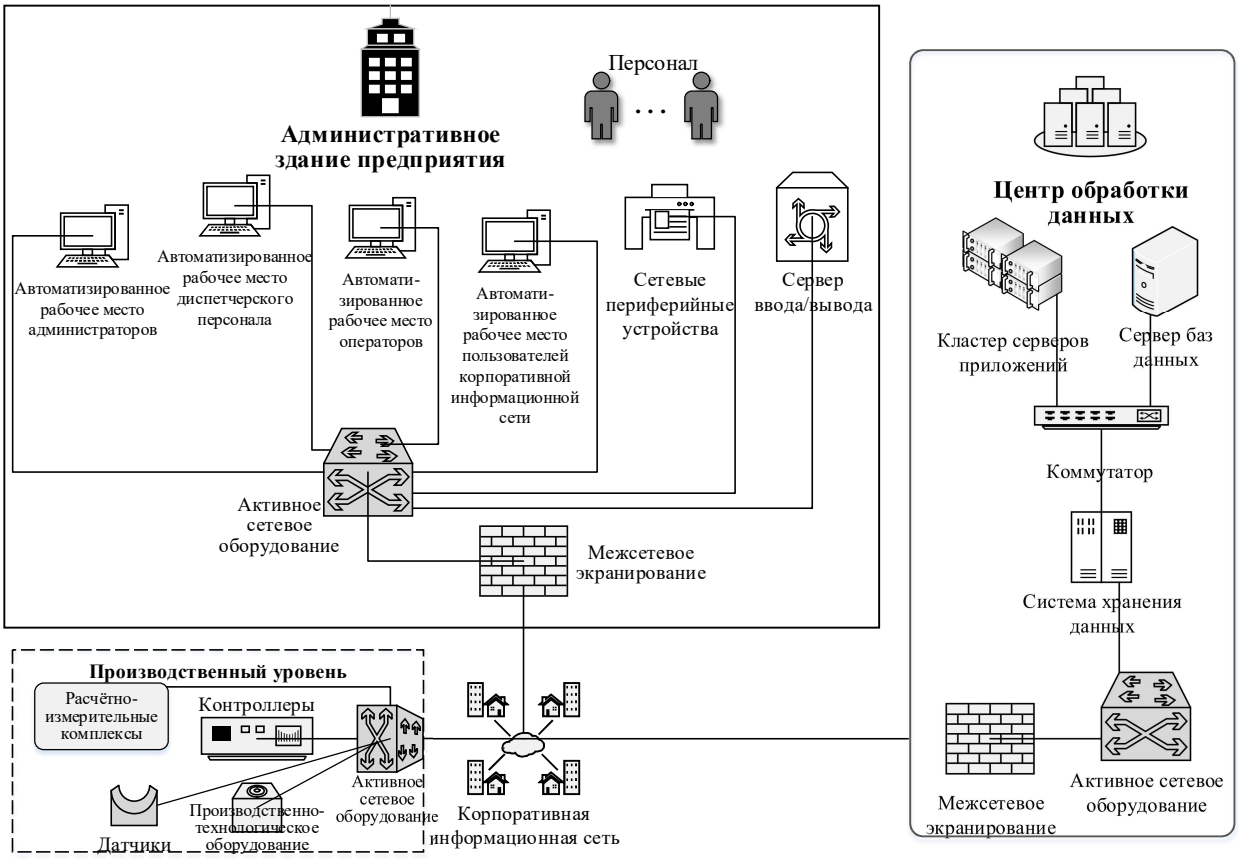

Рисунок 1 – Типичная архитектура промышленных информационных систем (составлено автором)

Теоретические и прикладные исследования в сфере управления рисками безопасности промышленных ИС единичны и носят отрывочный характер. Актуализирует проблему исследования необходимость выполнения Федерального закона [8], в соответствии с которым промышленные ИС являются объектами критической информационной инфраструктуры Российской Федерации. Риски безопасности промышленных ИС способны нанести ущербы или убытки, привести к остановке БП предприятия.

Учитывая вышеизложенное, сделаем вывод о существовании необходимости углубленного исследования данного аспекта. К промышленным ИС предъявляются высокие требования к обеспечению ИБ и управлению рисками безопасности [2, 7]. Это обуславливается направлениями задач, которые решаются такими системами, и негативные последствия, к которым могут привести риски безопасности. Таким образом, промышленные ИС имеют очень сложное строение, выбор средств управления рисками должен осуществляться исходя из рациональности их применения совместно со средствами защиты информации. Для промышленных ИС существует высокое число угроз и уязвимостей специфичного характера, поэтому преимущественным при проектировании архитектур СЗИ является технология эшелонированной защиты [2, 3].

В качестве решения исследуемой проблемы предложен метод управления рисками безопасности в таких системах (рисунок 2).

Рисунок 2 – Метод управления рисками безопасности в промышленных информационных системах (собственные разработки автора)

Метод управления рисками безопасности в промышленных ИС спроектирован в виде шести процедур. Каждая процедура реализует задачи управления рисками безопасности. Выявленные проблемы управления рисками безопасности указывают на высокую сложность данного процесса, реализация которого не может основана на системном анализе (СА). Так в данном методе СА выполняется на процедуре «Определение области применения рисков», в результате проведения которой будет исследована не только промышленная ИС, но и информационные ресурсы и БП ПП.

Данные результаты позволят классифицировать риски безопасности и сформировать критерии оценки рисков. Сведения, полученные при выполнении первой процедуре позволять выполнить комплексные анализ угроз промышленных ИС. Оценка и обработка рисков выполняются как до внедрения в ПП средств защиты информации (СЗИ), так и после (или после их обновления). Процедура «Мониторинг и переоценка рисков» обеспечивает отслеживание изменения рисков в режиме реального времени, а также динамику факторов рис-

ков. Процедура «Выбор защитных механизмов» учитывает не только стадии жизненного цикла промышленной ИС, но и возможности проектно-плановой деятельности по обеспечению информационной безопасности ПП (лицензирование, аттестацию, пилотный проект, рекомендации развития и совершенствования систем защиты информации).

Литература

1. АСКОН СТРЕМЛЕНИЕ Спецвыпуск АСКОН для ОПК [Электронный ресурс]: Корпоративный журнал компании АСКОН. 2016. №1 (17). 76 с. https://ascon.ru/source/info_materials/ascon_corporate_magazine_17.pdf.

2. Коробейников А.Г., Трояков И.Б., Жаринов И.О. Методы и модели оценки инфраструктуры системы защиты информации в корпоративных сетях промышленных предприятий: монография / Под ред. П.П. Парамонова, СПб: Изд-во ООО «Студия «НП-Принт». 2012. 115 с.

3. Козунова С.С., Бабенко А.А. Information security model in the segment of corporate information system // Информационные системы и технологии. 2017. №1 (99). С.87-91.

4. Рычков Д.В. О проблемах информационная безопасность на производстве // Автоматизация в промышленности. 2020. №7.

5. Бабенко А.А., Козунова С.С. Модель оценки и прогнозирования рисков инвестирования информационной безопасности промышленных предприятий [Электронный ресурс] // Научный результат. Сер. Информационные технологии : сетевой научно-практический журнал. - 2016. - Т. 1, № 4. - 29-35. – Режим доступа : http://research-result.ru/media/information/2016/4/5_it.pdf.

6. Кусакина Н.М. Применение анализа больших данных в информационной безопасности [Электронный ресурс] // Перспективные информационные технологии (ПИТ-2020): труды Международной научно-технической конференции (г. Самара, 21-22 апреля 2020 г.) / под ред. С.А. Прохорова. – Самара, Издательство Самарского научного центра РАН, 2020. – С. 183-187. – Режим доступа : https://ssau.ru/pagefiles/sbornik_pit_2020.pdf.

7. Козунова С.С., Черников Б.В., Черникова Е.А. Управление информационными рисками в информационных системах конструкторского бюро // Информатизация и связь. 2020. №6. С.17-20.

8. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 N 187-ФЗ.