УДК 004.056
DOI: 10.33764/2618-981X-2019-6-2-86-91

ПЛАНИРОВАНИЕ И РАЗРАБОТКА КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ОБОРОННО-ПРОМЫШЛЕННОГО КОМПЛЕКСА

Муратжан Бактыярович Шакиров
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант, тел. (923)134-54-10, e-mail: murat_shakirov@mail.ru

Игорь Николаевич Карманов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент, зав. кафедрой информационной безопасности, тел. (903)937-27-90, e-mail: i.n.karmanov@ssga.ru

Продемонстрирована важность комплексной системы безопасности на предприятиях оборонно-промышленного комплекса. Приведены описание, недостатки и преимущества существующей системы безопасности в данных организациях. Предложен комплексный подход к созданию системы обеспечения безопасности. Проанализирована роль комплексной системы безопасности на предприятии оборонно-промышленного комплекса. Показана актуальность рассматриваемой темы для предприятия и государства в целом.

Ключевые слова: оборонно-промышленный комплекс, комплексная система безопасности предприятия, интегрированные системы безопасности, информационная безопасность, национальная безопасность, фрагментарный подход, комплексный подход.

PLANNING AND DEVELOPMENT OF COMPREHENSIVE SECURITY SYSTEM OF MILITARY-INDUSTRIAL COMPLEX ENTERPRISE

Muratzhan B. Shakirov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, phone: (923)134-54-10, e-mail: murat_shakirov@mail.ru

Igor N. Karmanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Head of Department of Information Security, phone: (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

The importance of integrated security system at military-industrial complex enterprises is demonstrated. The article describes disadvantages and advantages of existing security system in such organizations. The complex approach to security system creation is offered. The role of integrated security system at military-industrial complex enterprise is analyzed. The relevance of considered topic for an enterprise and the state as a whole is shown.

Key words: military-industrial complex, complex security system of an enterprise, integrated security systems, information security, national security, fragmented approach, integrated approach.

Введение

Оборонно-промышленный комплекс (ОПК) – это комплекс отраслей, предприятий и организаций, составляющих специфический сектор экономики, который предназначен для удовлетворения военных потребностей государства.

Это одна из важнейших экономических систем в России, одна из целей данной системы – это решение проблем государства в области инновационного развития страны. Именно данной индустрии отдается приоритетное внимание при выполнении работ по созданию современных видов военной техники, производстве инновационных продуктов и технологий, выполнении перспективных прикладных и фундаментальных исследований и разработок, интеграции науки и производства.

Бесперебойная работа предприятий ОПК является залогом национальной безопасности. Любая авария, любой инцидент грозит не только человеческими потерями, но и материальным ущербом для предприятия. Длительные простои производственных мощностей могут разорвать цепь кооперации и сорвать деятельность государственной программы вооружений. Чтобы обеспечить бесперебойную работу предприятий военно-промышленного комплекса, необходимо спланировать и разработать комплексную систему безопасности. Все вышеперечисленное доказывает актуальность темы.

Необходимость укрепления обороноспособности российского государства в условиях ухудшения геополитической ситуации и важность удовлетворения потребностей гражданских отраслей в высокотехнологичной машиностроительной продукции отечественного производства на основе использования научно-производственного потенциала ОПК актуализируют проблему обеспечения безопасности предприятий комплекса [1–3].

Безопасность – это не только физическая безопасность предприятия, поскольку угрозами могут быть не только физическая потеря, повреждение или уничтожение имущества, но и такие факторы, как некомпетентность собственного персонала, нечестность конкурентов или партнеров, информационная война, изменения в экономической и/или геополитической ситуации и многое другое.

Безопасность предприятия является наиболее важным фактором, влияющим на функционирование предприятия. По этой причине увеличивается значимость и важность проблемы планирования и исследования комплексной системы безопасности для оборонных предприятий, отвечающей интересам не только самого предприятия, но и в целом страны. Сложные системы безопасности объединяют множество разных функций и снижают стоимость защиты объектов и обеспечения значимых бизнес-процессов.

Чтобы комплексная система безопасности предприятия ОПК дала положительный эффект, следует предварительно осуществить анализ и оценку безопасности с учетом всевозможных обстоятельств, оказывающих большое влияние на нее.

Методы обеспечения комплексной безопасности предприятия ОПК

Система комплексной безопасности включает в себя все технические средства защиты; функциональные и интегрированные, автономные и централизованные системы, которые обеспечивают безопасность и защиту объекта по установленным для него показателям и уровню защиты.

Также в систему комплексной безопасности предприятия ОПК входят технические средства или системы, которые уведомляют о состоянии инженерного оборудования или систем жизнеобеспечения объекта, а в некоторых случаях защищают их от несанкционированного воздействия. К средствам технической защиты относятся действующие образцы детекторов, приборов, устройств, ретрансляторов и аналогичных продуктов, которые являются частью существующих систем охранной и пожарной сигнализации, передача уведомлений по используемым каналам связи, контроль и управление доступом, а также некоторые средства связи, охраны периметра, системы внутренней связи и инспекционные системы [4, 5].

Существуют два основных подхода к обеспечению безопасности предприятия: фрагментарный и комплексный. Фрагментарный подход фокусируется на конкретных объектах, представляющих угрозу предприятию, его действия имеют локальный характер. Данный подход необходим для защиты конкретных объектов от конкретных угроз. При комплексном подходе происходит интеграция разнообразных мер обеспечения безопасности в единую систему, что позволяет существенно расширить спектр предотвращаемых угроз защищаемому объекту.

В свою очередь, обеспечение безопасности любого предприятия подразумевает построение единого информационного пространства, содержащего в себе единую программно-аппаратную телекоммуникационную среду, обеспечивающую постоянный взаимообмен сведениями и соединяющую все без исключения информационные ресурсы предприятия. В настоящее время на первый план здесь выходят вопросы, связанные с обеспечением безопасности объектов критической информационной инфраструктуры (КИИ), к которым, безусловно, относятся любые информационные системы предприятий ОПК [6–8]. Основными задачами системы безопасности предприятия в данном контексте являются:

– предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом КИИ, ее уничтожения, модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

– недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта КИИ;

– восстановление функционирования предприятия ОПК, обеспечиваемое, в том числе, за счет создания и хранения резервных копий необходимой информации;

– взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Главной целью комплексной системы безопасности представляется обеспечение того, чтобы предприятие могло благополучно реализовывать собственную деятельность в условиях непостоянства внешней среды, вовремя распознавать любые возможные опасности с целью предотвращения их реализации, за-

щищать здоровье и жизнь работников, защищать свои интересы всеми легитимными методами.

Планирование и разработка системы комплексной безопасности предприятия

Планирование и разработка отдельных процессов системы безопасности, осуществляемых с помощью специализированных программно-аппаратных комплексов, позволяют выбрать и проверить пути совершенствования с максимальным приближением к реальности до внедрения на предприятии военно-промышленного комплекса. Формирование единого информационного пространства позволяет объединить технические средства и системы, обеспечивающие безопасность предприятия, тем самым обеспечивая возможность быстрого реагирования на возможные инциденты. Таким образом, создание интегрированной системы безопасности невозможно без процесса планирования и развития ее отдельных элементов [9, 10].

Комплексная система безопасности предприятия ОПК необходима для выявления реальных и прогнозирования потенциальных опасностей и угроз, поиска методов их избегания, ослабления либо ликвидации результатов их влияния, поиска сил и средств, требуемых для обеспечения безопасности предприятия, организации взаимодействия с правоохранительными и контрольными органами в целях предотвращения и подавления правонарушений, нацеленных против интересов предприятия, своевременной адаптации к актуальным угрозам безопасности предприятия. На физическом уровне служба безопасности может содержать следующие отделы, группы, подразделения: охраны, инженерно-технической защиты, информационно-аналитической деятельности, своевременного реагирования и т. д. При этом гарантируется пожарная безопасность, сохранность имущества, предотвращается несанкционированный доступ на объект. С помощью организационных мер формируются специализированные подразделения, посты, патрули, зоны защищенности. Кроме того, компонентами структуры могут быть подразделения компании, активно участвующие в обеспечении единой безопасности (кадровое, финансовое, плановое, юридическое).

Результаты

Планирование и разработка комплексной системы безопасности предприятия ОПК должны основываться на следующих принципах:

1) сложность (комплексное применение правовых, организационных и инженерно-технических мер);

2) своевременность (анализ и прогнозирование ситуации, угроз безопасности предприятия, принятие эффективных мер по их предотвращению);

3) непрерывность;

4) законность (меры безопасности должны соответствовать законодательству Российской Федерации);

5) экономическая целесообразность (разумное соотношение между предполагаемыми потерями от угроз и затратами на их предотвращение);

6) специализация (создание на предприятии отделов и служб по защите информации, привлечение к разработке и реализации мер по защите интересов предприятия организаций, специализирующихся в конкретной области деятельности по обеспечению безопасности и имеющих опыт успешно реализованных проектов);

7) взаимодействие и координация (взаимодействие подразделений и служб предприятия в процессе внедрения мер обеспечения безопасности).

Заключение

Таким образом, для обеспечения безопасности предприятий оборонной промышленности необходимо реализовать целый комплекс мер по предотвращению воздействия угроз различного характера. Также необходимо полностью интегрировать систему безопасности с другими системами предприятия, обеспечив ее функционирование.

Планирование и разработка комплексной системы безопасности предприятия оборонно-промышленного комплекса является важным не только для экономики или самого предприятия, а для государства в целом. В связи с непрерывным развитием технологий необходимо совершенствовать системы безопасности предприятий оборонно-промышленного комплекса в соответствии с требованиями текущего времени.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Барышева О. С. Экономическая безопасность предприятий оборонно-промышленного комплекса // Экономика и менеджмент инновационных технологий. – 2017. – № 1 [Электронный ресурс]. – Режим доступа: http://ekonomika.snauka.ru/2017/01/13263 (дата обращения: 20.03.2019).

2. Бочуров А. А., Курбанов А. Х. Перспективы и проблемы развития отечественного оборонно-промышленного комплекса в современных условиях [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/perspektivy-i-problemy-razvitiya-otechestvennogo-oboronno-promyshlennogo-kompleksa-v-sovremennyh-usloviyah (дата обращения 11.03.2019).

3. Вертакова Ю. В., Плотникова Н. А., Плотников В. А. Промышленная политика России: направленность и инструментарий // Экономическое возрождение России. – 2017. – № 3 (53). – С. 49–56.

4. Интегрированный комплекс инженерно-технических средств охраны и системы контроля и управления доступом / Д. Е. Демидов, В. Н. Легкий, И. Д. Фисун, А. Р. Читава // Интерэкспо ГЕО-Сибирь. XIV Междунар. науч. конгр. : Междунар. науч. конф. «Наука. Оборона. Безопасность-2018» : сб. материалов (Новосибирск, 23–27 апреля 2018 г.). – Новосибирск : СГУГиТ, 2018. – С. 7–12.

5. Сафиханов А. А., Козин М. Н., Курбанов Т. Х. Национальные интересы России в Арктической зоне Российской Федерации: военно-экономический аспект. // Вестник Забайкальского государственного университета. – 2016. – № 11. – С. 125–139.

6. Оюн Ч. О., Попантонопуло Е. В. Объекты критической информационной инфраструктуры // Интерэкспо ГЕО-Сибирь. XIV Междунар. науч. конгр. : Магистерская научная сес-

сия «Первые шаги в науке» : сб. материалов (Новосибирск, 23–27 апреля 2018 г.). – Новосибирск : СГУГиТ, 2018. – С. 45–49.

7. Кульбякина Н. Д., Сырецкий Г. А., Макарова Д. Г. Безопасность автоматизированной системы управления технологическим процессом приборостроительного предприятия в контексте 187-ФЗ // Актуальные проблемы оптотехники [Текст] : сб. материалов Национальной научно-технической конференции, 22 октября 2018 г., Новосибирск. – Новосибирск : СГУГиТ, 2018. – С. 98–101.

8. Дворникова О. А., Макарова Д. Г. Защита изделий двойного назначения при их разработке и эксплуатации в контексте ФЗ-187 // Актуальные проблемы оптотехники [Текст] : сб. материалов Национальной научно-технической конференции, 22 октября 2018 г., Новосибирск. – Новосибирск : СГУГиТ, 2018. – С. 88–91.

9. Петухов Р. Н. Обеспечение безопасности на промышленных предприятиях [Электронный ресурс] // Молодой ученый. – 2016. – № 1. – С. 455–458. – Режим доступа: https://moluch.ru/archive/105/24979/ (дата обращения: 22.03.2019).

10. Плотников В. А., Курбанов А. Х., Князьнеделин Р. А. Государственный заказ как инструмент промышленной политики в оборонно-промышленном комплексе: теория и практика. – СПб. : Копи-Р Групп, 2013. – № 4. – С. 18–22.