Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Приходько Е.С. Вариант создания и организации работы комплексной системы обеспечения безопасности предприятия // Академия педагогических идей «Новация». – 2018. – №5 (май). – АРТ 166-эл. – 0,2 п. л. – URL: http://akademnova.ru/page/875548

РУБРИКА: ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

УДК 331

Приходько Екатерина Сергеевна
Студент «Электромеханического факультета»
Омский Государственный университет Путей Сообщения
г. Омск Российская Федерация
e-mail: ekaterina_prikhodko@list.ru

ВАРИАНТ СОЗДАНИЯ И ОРГАНИЗАЦИИ РАБОТЫ КОМПЛЕКСНОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Аннотация: Статья посвящена созданию оптимального варианта для обеспечения безопасности, а так же совершенствованию способов защиты предприятия.

Ключевые слова: система, элементы, защита, безопасность, КСОБП.

Prikhodko Ekaterina Sergeevna
Student of the Electromechanical Faculty
Omsk State University of Communications
Omsk Russian Federation

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

OPTION FOR THE ESTABLISHMENT AND ORGANIZATION OF THE WORK OF THE COMPLEX SYSTEM OF ENSURING THE ENTERPRISE SAFETY

Abstract: The article is devoted to the creation of the optimal variant for ensuring security, as well as improving the ways of protecting the enterprise.

Key words: system, elements, protection, safety, COSOB.

В 21 веке современный рынок предлагает огромное количество решений для проблем обеспечения безопасности предприятия. Вариативность решений представляются в виде проектов, которые производятся специальными компаниями, деятельность этих компаний заключается в консультировании производителей. Необходимость обеспечения безопасности бизнеса диктует совершенствование способов его защиты. Выбор различных технологий и систем для обеспечения безопасности, каждый бизнесмен выбирает сам. В итоге, каждому владельцу предприятия требуется четкое представление, как будет осуществляться защита его прав и собственности.

Актуальность проблемы подтверждается низкой активностью бизнес - сообщества, его неспособностью оперативно реагировать на вызовы, сохраняя безопасность своей деятельности. Предлагаем рассмотреть вариант создания комплексных систем обеспечения безопасности предприятия (далее по тексту КСОБП).

Рассмотрим элементы, составляющие терминологию КСОБП.

1)Одним из основных элементов данной системы является – комплекс. Основное его назначение объединять в себе элементы одной системы, отвечающие за какой - либо процесс, для решения одной единой цели.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

2)Система как элемент КСОБП очень важна. Под системой мы понимаем совокупность составляющих компонентов, которые зависят друг от друга. Компоненты, которые взаимодействуя между собой способны образовать единое целое.

3)Не менее важным элементом является - безопасность. В современном мире ни одна система, ни одно предприятие и т.д. не обходится без защиты. Под безопасностью мы понимаем защищенность объекта от разных факторов воздействия, не способность вредителей нарушить порядок и устроить разлад сложившейся системы.

4) Еще один элемент КСОБП это, непосредственно, предприятие. Предприятие собирает в себе все выше перечисленные элементы, с их помощью она осуществляет свою деятельность, производит товары, предоставляет услуги и т.д.

Анализ терминологии элементов, составляющий КСОБП, подтвердил их тривиальность. Главное для создания и организации КСОБП заключается в том, чтобы каждый руководитель осознавал всю важность проблемы безопасности своего предприятия. В связи с этим, важно, подготовить систему, в которой будут работать все элементы, при которых она, в свою очередь, будет сообразно реагировать на разные опасности, риски и угрозы. Многолетний опыт показывает, что такую систему создать вполне реально!

Например, еще в 2007 году на машиностроительном комплексе – одном из самых больших и трудных по структуре отраслей промышленности Поволжья внедрили совокупный подход к работе системы безопасности, что в дальнейшем заметно снизило убытки предприятия.

Прошло почти десять лет. Сегодня существует множество способов обезопасить свое предприятия. Это могут быть и услуги охранного агентства, либо камеры видео наблюдения и т.д. Безусловно, все эти способы

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

помогают обезопасить предприятие от злоумышленников, но если все эти средства объединить в одно целое, то можно получить большой функционирующий организм по обеспечению безопасности.

Для начала необходимо осуществить проверку безопасности, организовав собственную проверку вашего предприятия, воспользовавшись тестом на проникновение. А именно: допустим, в любой рабочий день, специально обученный сотрудник, попытается под придуманной историей попасть на территорию вашего предприятия, при этом он должен постараться пробыть там как можно дольше, для того, чтобы собрать какую-либо информации собирать и о вашем предприятии. Вам, необходимо будет проконтролировать время реакции системы безопасности на такую ситуацию.

Следующим тестом может выступить тест на взлом внутренней системы (базы) предприятия. Сейчас большой популярностью пользуется работа компьютерных злоумышленников, вашу информацию похитят молниеносно. Смогут ли заметить такой взлом ваши работники?

И, наконец, третий тест на инцидентную уязвимость. На данный момент террористические проявления стали очень частыми событиями, и их нельзя исключать. Подумайте, какие места на вашем предприятии может полностью вывести его из строя. Организуйте попытку доступа к этим местам специального человека, которые сделает модель диверсии.

Если руководитель по разным причинам не может осуществить проверку предприятия, то данное поручение можно передать экспертам в данной области. После такого ряда проверок результат будет известен только руководителю, так же как и дополнительные рекомендации по выявившимся проблемам.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Следующим этапом могло бы стать выявление и анализ рисков, угроз, которые создают проблему для существования вашего предприятия в данный момент. Риски, как и угрозы, имеют схожий характер. Но меняется время, меняются технологии, и появляются новые угрозы, поэтому ваша система безопасности должна идти в ногу со временем. И всё же, объектом постоянного наблюдения должны быть - сами угрозы.

Очередным мероприятием является собственно сама процедура реализации собственной КСОБН, после добавления в неё всех нужных элементов.

Для того чтобы реализовать данную систему конечно же должен быть человек который будет руководить ей, а именно руководитель. Так же будет уместно создать отдел по безопасности, которым и будет командовать руководитель. Как и в любом функционирующем отделе должна присутствовать рабочая техника. Для более продуктивной работы необходим штат специалистов, между которыми будут распределены обязанности. Ну и, конечно же, для хорошей работы данного отдела и системы в целом пригодятся ресурсы и привлекаемые сторонние силы.

Все это поможет вам управлять всей структурой обеспечения безопасности вашего предприятия.

Четвертым действием является формулировка условий оценивания эффективности работы КСОБП. Данный вопрос сложен по своей сути, так как у каждой системы свой критерий оценивания. Задачей каждого критерия является оценка реакции системы на существующую опасность или угрозу в настоящее время. Традиционно используют следующие виды условий оценки:

• квантитативный (сколько произошло инцидентов за определенный промежуток времени);

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

• квалитативный (убытки уменьшились, доходы увеличились);
• компаративный (сходство с опытом прошлых лет).

Пятым шагом является проведение необходимой модернизацию КСОБП. Можно задать вопрос «Можно ли создать модель безопасности, которая будет исключать все потери фирмы?» Наиболее часто звучит отрицательный ответ. Однако эти убытки можно свести до определенного уровня, чтобы предприятие имело хороший доход.

Таким образом, вариантов создания и организации работы КСОБП множество. Но безопасность вашего предприятия зависит только от вас, от того на сколько серьезно и ответственно вы подойдете к решению данной проблемы.

Список использованной литературы:

1. Алексенцев А. И. Понятие и назначение комплексной системы защиты информации. — 1996.
2. . Гришина К. В. Моделирование угроз конфиденциальной информации — 2001.
3. . Крысин А. В. Безопасность предпринимательской деятельности. — М.: Финансы и статистика, 1996.
4. . http://dic.academic.ru/dic.nsf/enc2p/3536185.
5. . http://base.garant.ru/70309010/

Дата поступления в редакцию: 26.05.2018 г.
Опубликовано: 31.05.2018 г.

© Академия педагогических идей «Новация», электронный журнал, 2018
© Приходько Е.С., 2018