

МОДЕЛИ ОРГАНИЗАЦИОННОГО УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Светлана Вячеславовна Рязанова

Сибирский государственный университет геосистем и технологий, 630102, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, тел.(383)343-91-11, e-mail: ryazanovaass@gmail.com

Аэлита Владимировна Шабурова

Сибирский государственный университет геосистем и технологий, 630102, Россия, г. Новосибирск, ул. Плахотного, 10, доктор экономических наук, директор Института оптики и технологий информационной безопасности, зав. кафедрой фотоники и приборостроения, тел.(383)344-40-58, e-mail: aelita_shaburova@mail.ru

Организационные аспекты в информационной безопасности являются одним из ее важнейших элементов, так как от их реализации в значительной степени зависит эффективность и результативность всей деятельности организации на должном уровне. В настоящее время не существует единой модели, которая подходила бы каждому предприятию и соответствовала их внутренним требованиям. В данной статье рассмотрены несколько моделей управления информационной безопасностью, а также общая модель организационного управления. Управление подразделяется на централизованное и децентрализованное. Рассмотрены преимущества и недостатки моделей для предприятий с разными потребностями. При выборе конкретной модели необходимо учитывать размеры, деятельность организации и финансовые возможности. При этом, крупным предприятиям выгодней выбирать централизованное управление, а для малых – децентрализованное.

Ключевые слова: информационная безопасность, модель организационного управления информационной безопасностью, централизованное управление, децентрализованное управление.

MODELS OF ORGANIZATIONAL MANAGEMENT OF INFORMATION SECURITY

Svetlana V. Ryazanova

Siberian State University of Geosystems and Technologies, 10 Plakhotnogo St., Novosibirsk, 630102, Russia, Graduate, Department of Photonics and Device Engineering, phone: (383)343-91-11, e-mail: ryazanovaass@gmail.com

Aelita V. Shaburova

Siberian State University of Geosystems and Technologies, 10 Plakhotnogo St., Novosibirsk, 630102, Russia, D.Sc., of Economics, Director of the Institute of Optics and Information Security Technologies, Head of the Department of Photonics and Device Engineering, phone: (383)344-40-58, e-mail: aelita_shaburova@mail.ru

The article provides several security models. All models have access to the target. When choosing a specific model, it is necessary to take into account that management is divided into centralized and decentralized. The scheme of the model of organizational management of open security is considered.

Key words: information security, model of organizational management of information security, centralized management, decentralized management.

Введение

Роль организационного аспекта управления информационной безопасностью возрастает по мере роста уровня зрелости процессов обеспечения информационной безопасности (далее ОИБ) в организации. Каждая организация нуждается в надежном механизме защиты информации на административно-правовом уровне и организационной основе, что исключало бы (или сводило к минимуму) возможность возникновения опасности доступа к информации. Поэтому, модели организационного управления информационной безопасностью (далее ИБ) является актуальной для каждой организации.

Организационное управление ИБ определяет способ, которым ИБ передается под контроль, реализуется и управляется во всей организации. Это достигается за счет определения и классификации существующей в организации структуры как соответствующей определенному типу управления ИБ, а также выяснения того, могут ли потребности организации быть удовлетворены путем использования всех преимуществ ИБ в рамках данного типа управления.

Методы и материалы

На данный момент не существует единого подхода к организационному управлению ИБ, но возможно выделить его классическую модель, которая представлена на рис. 1. Для использования такой модели, организация сначала определяет потребности в ОИБ и вид управления ИБ, требуемый в настоящее время. Затем разрабатывается стратегия ОИБ организации, учитывающая тип управления ИБ и потребностей в ОИБ. После определения стратегии и осуществления выбора эффективного типа управления ИБ приступают к разработке архитектуры ОИБ в рамках имеющейся организационной структуры. Если стратегия не актуальна, то необходимо что-то изменить. Самым простым подходом будет пересмотреть стратегию. Если же это невозможно, то приступают к модификации руководства ИБ или руководства и администрирования.

Основываясь на том, что организационное управление ИБ заключается в двух основных видах деятельности – руководство и администрировании (которые в свою очередь могут быть централизованными или децентрализованными), и проанализировав их, необходимо ввести следующие термины:

– централизованное руководство (ЦР) указывает на такую организацию руководства, при которой полномочия по принятию решений в области политики и бюджета, распространяемые на всю организацию, предоставляются одному представителю или собранию;

– централизованное администрирование (ЦА) предоставляет органу управления право применять и управлять политикой информационной безопасности управленческому персоналу ИБ или систем, которые последовательно подчинены друг другу [8];

– децентрализованное руководство (ДА) предоставляют органу управления право применять и управлять политикой информационной безопасности управленческому персоналу, который имеет несколько цепочек подчиненности;

– децентрализованное руководство (ДР) указывает на то, что ни один человек или орган не уполномочен формулировать политику информационной безопасности и разрабатывать бюджет для деятельности в области ИБ.



Рис. 1. Модель организационного управления ИБ

Данные понятия могут комбинироваться между собой и на этой основе можно разработать несколько типов моделей организационного управления ИБ. Рассмотрим каждую модель в отдельности.

Результаты

Базовыми типами моделей являются модели централизованное руководство/централизованное управление и децентрализованное руководство/децентрализованное администрирование. Модель централизованного руководства/централизованного администрирования ИБ соответствует полной централизации всей деятельности в области ИБ. Она представляет такую организацию руководства, при которой полномочия по принятию решений в области политики и бюджета, распространяемые на всю организацию, предоставляются одному представителю или собранию. Одно лицо из высшего руководства отвечает за разработку политик, применяемых во всей организации. Персонал в рамках одной цепочки подчиненности выполняет все административные функции по управлению ИБ. Все подразделения делегируют своих представителей в комитет по управлению вопросами ИБ [5]. При использовании этого типа модели можно отметить следующие преимущества:

– один канал связи (повышение вероятности предотвращения утечки

информации);

- личная ответственность руководителя (повышение контроль качества действий подразделения);

- оперативность в принятии решений (повышение производительности предприятия).

Недостатки:

- перегрузка руководителя информацией, множество контактов с подчинёнными, вышестоящими структурами (с точки зрения несанкционированного доступа к информации, руководитель - самое слабое звено. Через него легко осуществить доступ к полной информации подразделения);

- концентрация власти в верхних ветвях системы управления (осуществив несанкционированный доступ к одному из главных руководителей, можно вывести из строя всю ветвь, следующую за ним, либо получить практически всю информацию по предприятию);

- затруднительные связи между инстанциями (приводит к долгому и неполному обмену информацией).

В свою очередь, модель децентрализованного управления/децентрализованного администрирования предполагает использование аутсорсинга, при этом этим внешним компаниям передается абсолютно все управление, т.е. финансовый детектор управляет контактом из аутсорсинговых финансовых компаний, директор по кадрам – аутсорсинговым кадровым агентством и т.д. Эта модель, в основном подходит для малых организаций, которые не имеют ресурсов для создания управляющего комитета по вопросам ИБ и не могут обслуживать свои информационные технологии самостоятельно. Внешние организации аутсорсинга отвечают за политики и процедуры, которые они применяют к своим ИТ-системам [7]. При этом тип децентрализованное руководство с децентрализованным управлением, пользуясь услугами аутсорсинга, имеет свои преимущества, такие как поддержка в режиме 24/7, привлечение узкопрофильных специалистов, отсутствие нехватки штата сотрудников и сокращение издержек на ОИБ [6].

Но многие организации вынуждены использовать сразу два атрибута для достижения целей ОИБ экономически эффективным образом, поэтому они в одно и то же время централизованные и децентрализованные. В этом случае появляются модели децентрализованное руководство/централизованное администрирование и централизованное руководство/децентрализованное администрирование. Рассмотрим эти типы моделей организационного управления ИБ.

Для типа децентрализованное руководство/централизованное администрирование характерно наличие нескольких лиц, ответственных за разработку политик в рамках их зон ответственности [2]. Эти политики передаются соответствующим администраторам для исполнения. Персонал подчиняется Управляющему директору и выполняет администрирование ИБ. Удаленные администраторы могут заключать соглашения, по которым обслуживание информационных технологий передается третьей стороне (аутсорсинг). Преимущество этого типа в том, что организация оставляет за собой право собственности и некоторые меры руководства ИТ-активами [6]. Этот тип особенно подходит для малых организаций, которые не имеют больших ресурсов для создания Управляющего комитета.

Если организация более крупная, то стоит использовать тип централизованное руководство/децентрализованное администрирование. В этом случае управление остается таким же, как при типе централизованное управление/централизованное администрирование, но отношения между службами ИБ существенно меняются, администраторы ИТ могут управлять обслуживанием ИБ и ИТ, а директор службы ИБ может иметь руководство над персоналом службы ИБ на некоторых удаленных объектах, но при этом не существует центральной точки руководства всем обслуживаемым ИБ.

Заключение

Проанализировав методы управления ИБ, можно сделать вывод, что для больших компаний больше подходит централизованное управление, для малых - децентрализованное.

Централизация указывает на наличие единого органа, который может быть отдельным лицом, комитетом или другой структурной единицей, а децентрализация подразумевает наличие нескольких органов с одинаковым уровнем полномочий.

Таким образом, преимущества и недостатки каждого типа управления ИБ будут различны для разных организаций. Базовая модель организационного управления позволяют выбрать более подходящий организации тип управления и сделать его самым эффективным и экономически выгодным. В целом, при выборе модели организационного управления необходимо учитывать соответствие нормативно-правовой базе, экономические возможности компании и ее потребности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Tipton H. F., Krause M. Information Security Management Handbook. Taylor & Francis Group, USA, 2007.
2. А. А. Парошин Нормативно-правовые аспекты защиты информации. Выпуск 4 : учебное пособие / А. А. Парошин. — М.; ДФУ, 2017. — 218 с.
3. Басыня, Е.А. Системное администрирование и информационная безопасность. учебное пособие – Новосибирск: НГТУ, 2018. — 79 с.
4. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.и. Основы управления информационной безопасностью: учебное пособие для вузов. М.: Горячая линия-Телеком, 2012. – 45с
5. Обеспечение информационной безопасности бизнеса / Под ред. А.П. Курило. – М.: Альпина Паблшерз, 2011. – 86 с.
6. Бирюков, А.А. Информационная безопасность: защита и нападение – М.: ДМК Пресс, 2017. – 256 с.
7. Варфоломеев А.А. Основы информационной безопасности. учебное пособие. –М. : РУДН, 2008. - 412 с.
8. Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации: учебное пособие. – Санкт-Петербург: Университет ИТМО, 2018. - 56 с.
9. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью». Выпуск 4 : учебное пособие. – М.: Горячая линия-Телеком, 2012.– 214 с.
10. Нестеров, С.А. Основы информационной безопасности: учебное пособие. – М.: Лань, 2013.– 324 с.

© С. В. Рязанова, А. В. Шабурова, 2020