Управление информационной безопасностью в корпоративной предпринимательской среде в условиях киберугроз цифровой экономики

Гасанов Эдуард Сарифович,
аспирант кафедры финансы и кредит Уфимского государственного нефтяного технического университета, fk@rusoil.net

Самарина Евгения Аликовна,
к.э.н., доцент кафедры финансы и кредит Уфимского государственного нефтяного технического университета, ev.samarina90@yandex.ru

В статье исследуются вопросы управления информационной безопасностью в корпоративной предпринимательской среде в условиях активного становления и развития цифровой экономики, сопровождающегося ростом киберугроз и киберпреступности в информационном пространстве.
Обеспечение информационной безопасности (ИБ) в современных условиях интенсивного развития цифровой экономики является одним из важнейших элементов корпоративного управления, поскольку в цифровую эпоху практически вся информация, которой оперирует компания, имеет ценность.
В условиях цифровой экономики информационную безопасность необходимо рассматривать как непрерывный, регламентированный и прогнозируемый процесс управления, тесно взаимоувязанный с целями и задачами бизнеса компании, охватывающий зоны ответственности широкого круга структурных подразделений, и управляемый непосредственно высшим руководством. Необходимо осуществить переход от защиты ресурсов, устройств и каналов связи к защите информации как таковой, и, в первую очередь ее разграничение на личную и корпоративную. Только при таком подходе возможно обеспечить сохранность и безопасность корпоративной информации ограниченного доступа (коммерческой, банковской, налоговой тайны) и иным ценным информационным активам компаний.
Ключевые слова: информационная безопасность, цифровая экономика, корпоративная предпринимательская среда, экономическая безопасность, киберугрозы, кибератаки, защита информации.

В государственной Программе «Цифровая экономика Российской Федерации» [7], развитие цифровой экономики определяется как приоритетная государственная задача, для решения которой одним из пяти приоритетных направлений определена информационная безопасность. Другими официальными документами, приоритезирующими задачу информационной безопасности на государственном уровне, являются «Стратегия развития информационного общества в Российской Федерации на 2017-2020 годы» [8], а также «Стратегия экономической безопасности Российской Федерации на период до 2030 года» [9]. Аналитический обзор указанных документов свидетельствует об осознании на правительственном уровне необходимости решения задач обеспечения информационной безопасности, которая находится в тесном сопряжении с экономической безопасностью страны и в условиях развития цифровой экономики требует к себе особо пристального внимания.

Количество обнародованных случаев утечки конфиденциальной информации ежегодно увеличивается в разы (что подтверждается данными аналитических отчетов Лаборатории Касперского [3, 4] и аналитического центра компании InfoWatch [1, 2]), при этом размер ущерба, понесенный компаниями в результате инцидента, увеличивается пропорционально их размерам. Если компании малого и среднего бизнеса терпят убытки в среднем порядка 1,6 млн. руб., то у крупных компаний ущерб существенно больше и составляет в среднем порядка 11 млн. руб. И это лишь усредненные цифры, причем, далеко не по всем кейсам, многие из которых в силу своих масштабов остаются закрытыми как предмет внутренних расследований, причем тем чаще, чем цифры больше [10].

По данным того же аналитического центра компании InfoWatch Россия занимает второе место по числу инцидентов утечки конфиденциальной информации. Данный факт обусловлен снижением на порядки стоимостью взлома доступа к корпоративной информации, в виду того что более половины участников корпоративного информационного обмена, в том числе 75% руководителей компаний широко используют потребительские устройства и неавторизированные приложения, в принципе не рассчитанные на работу в корпоративной информационной среде и при этом локально хранящие огромные объемы существенных корпоративных данных. Обмен служебной информацией как между руководителями, так и среди рядовых сотрудников осуществляется при помощи общедоступных потребительских сервисов (почтовых и файлообменников), несанкционированный доступ к которым – наиболее частый инцидент. А утечки специальных инструментов, подробно описанные Wikileaks, только повышают риски прямого доступа к информации, находящейся в обычных приложениях на смартфонах и планшетах руководителей всех

уровней, которые не имеют другой альтернативы. Доступ к информации осуществляется как правило с личных мобильных устройств и по наиболее быстрому и доступному каналу передачи сигнала.

Как указывается в одном из отчетов Лаборатории Касперского 91% зарубежных и 96% отечественных компаний из участвующих в опросе столкнулись с угрозами информационной безопасности. Для российских компаний, треть кибератак закончились потерей важной для бизнеса информации.

Наиболее значимыми киберугрозами мирового уровня в условиях цифровой экономики экспертами определяются:

вирусы, шпионское ПО и другие вредоносные программы – 61%;

спам – 56%;

фишинговые атаки – 36%;

сбои, вызванные проникновением в корпоративную сеть – 24%;

DDoS-fnfrb – 19% [11].

Типы внешних угроз, с которыми сталкивались российские компании, по данным исследований Лаборатории Касперского представлены на рис. 1.

Рис.1. Типы внешних угроз, с которыми сталкивались российские компании

Что касается потерь, понесенных в результате сбоев в системе безопасности, российские IT-специалисты чаще всего называли потери данных о платежах (13%), интеллектуальной собственности (13%), клиентских баз (12%) и информации о сотрудниках (12%) [11].

Среди российских компаний – 84% не считают свою компанию возможным объектом кибератак, а 60% уверены, что их корпоративные системы надежно защищены. И только 16% респондентов считают свою компанию объектом целевых кибератак.

Подавляющее большинство российских IT-специалистов и менеджеров хорошо осведомлены и прекрасно осознают уровень серьезности и опасности современных угроз информационной безопасности, тем не менее степень защиты бизнеса от киберугроз далека от идеала: либо уровень защиты компании не соответствует, либо выбранные меры не отвечают характеру опасности и серьезности возможных потерь для компании.

В условиях развития цифровой экономики задача обеспечения бесперебойной и четкой работы системы информационной безопасности является одной из приоритетных стратегических задач любого бизнеса. К сожалению, в нашей стране до настоящего времени наиболее распространен реактивный подход к управлению информационной безопасностью, который предполагает инвестирование в развитие системы защиты информации как реакцию на инцидент, в то время как более эффективным и действенным является проактивный подход к управлению, цель которого является предотвращение возникновения инцидентов.

Учитывая, что по прогнозам специалистов в цифровом мире киберугрозы станут одним из основных бизнес-рисков, управление информационной безопасностью целесообразно выстраивать на основе процессного подхода, ориентированного на стратегическую перспективу с превентивной направленностью.

Процессный подход к реактивному управлению информационной безопасностью предполагает реализацию жизненного цикла управления событиями и инцидентами, связанными с информационной безопасностью, в самом общем виде включающего следующую последовательность этапов:

1. Обнаружение киберугрозы;
2. Анализ данных о безопасности;
3. Регистрация инцидента;
4. Установление причин возникновения инцидента;
5. Реагирование на инцидент;
6. Выявление, оценка и ликвидация последствий инцидента;
7. Анализ результатов ликвидации последствий инцидента.

Неавтоматизированные методы реализации перечисленных задач управления информационной безопасностью в условиях большого объема данных и постоянно изменяющейся информационной среды являются неэффективными, что снижает или сводит на нет возможность оперативного контроля состояния защищенности и принятия персоналом обоснованных решений по снижению рисков информационной безопасности. В цифровом мире автоматизация процессов управления информационной безопасностью при использовании проактивного подхода к управлению является объективной необходимостью.

Для автоматизации любой из задач в рамках процессов управления информационной безопасностью необходимо собрать исходные данные из различных источников, в качестве которых могут выступать средства защиты информации, инфраструктурные элементы и корпоративные информационные системы. От качества и полноты исходных данных зависит очень многое, поэтому в процессе внедрения средств автоматизации процессов, как правило, вскрываются проблемы функционирования систем защиты информации (ложные срабатывания правил в SIEM, отсутствие результатов анализа защищенности для отдельных сегментов, различие в версиях используемого ПО, отсутствие актуальной информации об активах, сетевой топологии и т.п.).

После сбора данных в единую универсальную базу в составе системы требуется выполнить их программную обработку, целью которой является расчет ключевых показателей и наглядное представление сводной информации, поддерживающих принятие управленческих решений пользователями различных уровней (с учетом ролевой модели и матрицы разграничения доступа), либо подлежащих передаче в целевые системы.

При обработке данных учитываются следующие параметры:

целевые формы представления и передачи данных;

роль пользователя, для которого эти данные предназначены;

характеристики имеющихся в компании процессов по управлению информационной безопасностью – цели использования и срок хранения, контролируемые параметры защиты, частота и аудитория предоставления, целевые системы для выдачи данных.

Таким образом, средство автоматизации вскрывает следующий пласт проблем – выявляется реальный уровень зрелости процессов управления информационной безопасностью в компании, который значительно улучшается при внедрении средств автоматизации процессов управления ИБ, так как для настройки системы требуется согласовать и документально зафиксировать все основные процедуры и метрики целевых и смежных с ними процессов (например, управление обновлениями ПО при устранении выявленных уязвимостей).

На практике одним из первых этапов подготовки к автоматизации процессов управления информационной безопасностью является построение процесса управления информационными активами, которые представляют собой имеющиеся технические средства информационно- телекоммуникационной инфраструктуры компании (например: АРМ, серверы, сетевое оборудование) и информационные системы, базирующиеся на данных средствах. Наиболее важным активом, напрямую влияющим на функционирование информационных систем, является сетевая инфраструктура. Знание уровня ее защищенности и реального статуса функционирования необходимо как ИТ-, так и ИБ-подразделению.

Популярные и наиболее хорошо освоенные средства автоматизации процессов управления информационной безопасностью предоставляют либо первичную информацию о состоянии защищенности информационно-телекоммуникационной инфраструктуры и способах ее использования, либо возможности по реактивной обработке зарегистрированных событий и инцидентов, связанных с информационной безопасностью без учета возможности автоматического ранжирования обрабатываемых данных с учетом действующих конфигураций применяющихся технических средств защиты, модели угроз и оценки рисков.

Реализация данной задачи возможна путем создания (в рамках выделенной подсистемы) модели информационно-телекоммуникационной инфраструктуры, которая описывает все основные параметры системы, внутренние связи и каналы между ее компонентами, на основании чего предусматривается возможность осуществлять оценку соответствия параметров системы заданным параметрам информационной безопасности и выполнять проактивное моделирование негативных ситуационных инцидентов в отношении элементов информационной безопасности.

Создание модели позволит не только консолидировать данные об информационных активах, и выполнять проверку планирующихся изменений (например, в части изменения сетевого доступа), но и проводить эффективную приоритизацию уязвимостей с использованием процессов моделирования сетевых атак.

В виду большого объема разнородных данных, в настоящий момент все, либо выделенные процессы управления информационной безопасностью, не могут быть полностью автоматизированы. При этом значительная часть функций все равно будет выделена на выполнение специалистами подразделений ИТ и ИБ.

Также при всей привлекательности проактивного управления и идеи с его помощью предотвратить все инциденты до их возникновения, необходимо понимать, что это невозможно и неоправданно с позиций ресурсозатратности. Существуют инциденты, которые дешевле устранить по факту, чем предотвращать. Поэтому целесообразно находить и поддерживать разумный баланс между реактивным и проактивным управлением.

На рынке есть ряд продуктов, в которых решаются задачи автоматизации процессов управления информационной безопасностью, но их внедрение должно быть постепенным, последовательным, с адаптацией под требования конкретной компании и с применением заложенных производителем лучших практик. Результаты становятся видны уже на этапе внедрения, когда решаются проблемы с источниками данных, описываются или уточняются описания действующих процессов, а у пользователей появляется осознание важности и целей проводимой работы.

Подводя итог, хотелось бы отметить, что применение систем с возможностью моделирования различных негативных ситуаций угрожающих информационной безопасности, позволяет подготовиться к внедрению полноценной системы по автоматизации процессов управления ИБ и качественно повысить эффективность автоматизируемых процессов.

Использованные в данных системах подходы по моделированию информационно-технологической инфраструктуры, сетевых атак, а также проактивному управлению ИБ, на наш взгляд, являются перспективными. Подтверждением этого является и то, что, ряд существующих и разрабатываемых SIEM решений уже содержат или будут включать в свой состав функциональные компоненты по моделированию сетевой инфраструктуры и сетевых атак.

Литература

1. Глобальное исследование утечек конфиденциальной информации в первом полугодии 2019 года [Электронный ресурс] / Аналитический центр InfoWatch. 2019. Режим доступа: https://www.infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf?rel=1, свободный.

2. Утечки данных. Россия. 2018 год. [Электронный ресурс] / Аналитический центр InfoWatch. 2019. Режим доступа: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Russ_Report_2018.pdf?rel=1, свободный.

3. Ландшафт угроз для систем промышленной автоматизации. Первое полугодие 2019. [Текст] / Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky Lab ICS CERT). 2019. – 31 с.

4. Ready…Or not? Balancing future opportunities with future risks. A global survey into attitudes and opinions on IT security. / The Kaspersky Lab Global IT Risk Report. Kaspersky.co.uk/beready. URL: https://media.kaspersky.com/documents/business/brfwn/en/The-Kaspersky-Lab-Global-IT-Risk-Report_Kaspersky-Endpoint-Security-report.pdf.

5. The 2018 Year End Vulnerability QuickView Report / RBS — Risk Based Security. URL: https://pages.riskbasedsecurity.com/2018-ye-vulnerability-quickview-report.

6. Утечки данных [Электронный ресурс] / Tadviser. Государство. Бизнес. ИТ. Режим доступа: http://www.tadviser.ru/a/119166, свободный.

7. Программа «Цифровая экономика Российской Федерации» [Текст]. Утв. Распоряжением Правительства Российской Федерации от 28.07.2017. № 1632-р / Собрание законодательства Российской Федерации. М., 2017. – 7 августа № 32. Ст.5138.

8. Указ Президента РФ от 09.05.2017 №203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2020 годы» [Электронный ресурс] / Режим доступа: http://kremlin.ru/acts/bank/41919, свободный.

9. Указ Президента РФ от 13.05.2017 № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» [Электронный ресурс] / Режим доступа: http://kremlin.ru/acts/bank/41921, свободный.

10. Орлик С. Почему для корпоративной мобильности требуется «новая безопасность» [Электронный ресурс] / Forbes. Технологии. Кибербезопасность. 29.06.2017. Режим доступа: https://www.forbes.ru/tehnologii/346841-pochemu-dlya-korporativnoy-mobilnosti-trebuetsya-novaya-bezopasnost, свободный.

11. Безмалый В. Пути развития технологий защиты. Как изменится характер угроз [Электронный ресурс] / Windows IT Pro/RE. 2013. - №04. Режим доступа: http://www.osp.ru/winitpro/2013/04/13034909/, свободный.

12. Digitization of taxes as a top-priority direction of optimizing the taxation system in modern Russia / Popkova E.G., Zhuravleva I.A., Abramov S.A., Fetisova O.V., Popova E.V. Studies in Systems, Decision and Control. 2019. T. 182. C. 169-175.

Information security management in the corporate business environment in the context of cyber threats to the digital economy

Gasanov E.S., Samarina E.A.
Ufa state oil technical University

The article investigates the issues of information security management in the corporate business environment in the conditions of active formation and development of the digital economy, accompanied by the growth of cyberthreats and cybercrime in the information space.

Ensuring information security (IS) in modern conditions of intensive development of the digital economy is one of the most important elements of corporate governance, because in the digital age, almost all information, which operates the company, has value.

In the conditions of digital economy it is necessary to consider information security as continuous, regulated and predicted process of management, closely interconnected with the purposes and problems of business of the company, covering zones of responsibility of a wide range of structural divisions, and operated directly by the top management. It is necessary to carry out transition from protection of resources, devices and communication channels to protection of the information as such, and, first of all, its differentiation on personal and corporate. Only with this approach it is possible to ensure the safety and security of corporate information of limited access (commercial, banking and tax secrecy) and other valuable information assets of companies.

Keywords: information security, digital economy, corporate business environment, economic security, cyberthreats, cyberattacks, information protection.

References

1. Global study of confidential information leaks in the first half of 2019 [Electronic resource] / analytical center InfoWatch. 2019. Access mode: https://www.infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf?rel=1, free.
2. Data leaks. Russia. 2018. [Electronic resource] / Analytical center InfoWatch. 2019. Access mode: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Russ_Report_2018.pdf?rel=1, free.
3. The threat landscape for industrial automation systems. The first half of 2019. [Text] / Kaspersky Lab ICS CERT information security incident response Center for industrial infrastructure. 2019. - 31 p.
4. Ready…Or not? Balancing future opportunities with future risks. A global survey into attitudes and opinions on IT security. / The Kaspersky Lab Global IT Risk Report. Kaspersky.co.uk/beready. URL: https://media.kaspersky.com/documents/business/brfwn/en/The-Kaspersky-Lab-Global-IT-Risk-Report_Kaspersky-Endpoint-Security-report.pdf.
5. The 2018 Year End Vulnerability QuickView Report / RBS — Risk Based Security. URL: https://pages.riskbasedsecurity.com/2018-ye-vulnerability-quickview-report.
6. Data breaches [Electronic resource] / Tadviser. State. Business. It. Mode of access: http://www.tadviser.ru/a/119166 free.
7. Program " Digital economy of the Russian Federation "[Text]. UTV. By order of the Government of the Russian Federation No. 1632-R dated 28.07.2017 / Assembly of legislation of the Russian Federation, Moscow, 2017-August 7, No. 32, Article 5138.
8. Decree of the President of the Russian Federation of 09.05.2017 No. 203 "on The strategy for the development of the information society in the Russian Federation for 2017-2020" [Electronic resource] / access Mode: http://kremlin.ru/acts/bank/41919, free.
9. Decree of the President of the Russian Federation dated 13.05.2017 No. 208 "on the Strategy of economic security of the Russian Federation for the period up to 2030" [Electronic resource] / access Mode: http://kremlin.ru/acts/bank/41921, free.
10. Orlik S. Why "new security" is required for corporate mobility [Electronic resource] / Forbes. Technologies. Cybersecurity. 29.06.2017. Access mode: https://www.forbes.ru/tehnologii/346841-pochemu-dlya-korporativnoy-mobilnosti-trebuetsya-novaya-bezopasnost, free.
11. Bezmaly V. Ways of development of protection technologies. How to change the nature of threats [Electronic resource] / Windows IT Pro/RE. 2013. - №04. Access mode: http://www.osp.ru/winitpro/2013/04/13034909/, free.
12. Digitization of taxes as a top-priority direction of optimizing the taxation system in modern Russia / Popkova E.G., Zhuravleva I.A., Abramov S.A., Fetisova O.V., Popova E.V. Studies in Systems, Decision and Control. 2019. T. 182. C. 169-175.