УДК 004.056 + 657.631.6 Вестник УрФО № 1(31) / 2019, с. 53–56

Баранкова И. И., Михайлова У. В., Быкова Т. В.

DOI: 10.14529/secur190108

СЛОЖНОСТИ, ВОЗНИКАЮЩИЕ ПРИ ПРОВЕДЕНИИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

В данной статье рассмотрены основные принципы, цели и задачи проведения аудита информационной безопасности. В частности, описан общий подход к проведению аудита на предприятии. Рассмотрена важность правильного анализа принадлежности предприятия к объектам критической информационной инфраструктуры. Перечислены основные проблемы, возникающие при проведении аудита информационной безопасности на примере предприятия ООО «Машиностроительный завод «РИВС». Проанализирована статистика кибератак на промышленные предприятия в 2018 году.

Ключевые слова: *информация, безопасность, защита информации, аудит информационной безопасности, информационная безопасность предприятия.*

Barankova I. I., Mikhailova U. V., Bykova T. V.

DIFFICULTIES IN CONDUCTING AN INFORMATION SECURITY AUDIT IN AN ENTERPRISE

This article describes the basic principles, goals and objectives of the information security audit. In particular, it describes the general approach to conducting an audit at an enterprise. The importance of correct analysis of the enterprise's belonging to the objects of critical information infrastructure is considered. The main problems arising during the audit of information security are listed on the example of the enterprise "Machine-building plant "RIVS". Analyzed statistics of cyberattacks on industrial enterprises in 2018.

Keywords: *information, security, information protection, information security audit, information security of an enterprise.*

Аудит информационной безопасности – системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности предприятия в соответствии с определёнными критериями и показателями безопасности.

Актуальность аудита информационной безопасности обусловлена усилением зависимости успешности деятельности предприятия от корпоративной системы защиты информации и увеличением объема жизненно важных для предприятия данных, обрабатываемых в корпоративной информационной системе. По данным «Лаборатории Касперского» около половины компьютеров рос-

сийской промышленности столкнулись с киберугрозами в 2018 году. Киберпреступники, по мнению экспертов «Лаборатории», были просто вынуждены обратить внимание на промышленность, поскольку банки и финансовые организации постоянно усиливают системы защиты. В процентном отношении было атаковано около 48% компьютеров промышленных предприятий. В первую очередь, это системы автоматизированного управления технологическим процессом. Для примерно трети систем источником угроз стал интернет, 5% подвергались атакам через съемные носители, а 2% - посредством почтовых программ разного рода.

К основным целям аудита информационной безопасности предприятия можно отнести следующие:

• получение объективной и независимой оценки текущего состояния защищенности информационных ресурсов предприятия;

• получение максимальной отдачи от средств, инвестируемых в создание системы информационной безопасности;

• оценка возможного ущерба от несанкционированных действий;

• разработка требований к построению системы защиты информации;

• определение зон ответственности сотрудников подразделений;

• расчет необходимых ресурсов;

• разработка порядка и последовательности внедрения системы информационной безопасности.

Наиболее простым видом аудита защищенности ИТ-инфраструктуры является сканирование на наличие уязвимостей, осуществляемое с помощью специального программного обеспечения [1]. Данный вид аудита позволяет выявить большинство известных уязвимостей в информационных ресурсах и получить детальные рекомендации по их устранению.

Поиск уязвимостей является одним из этапов тестирования на возможность несанкционированного проникновения, которое представляет собой имитацию действий злоумышленников по проникновению в корпоративную систему.

Различают внешнее тестирование на проникновение, в ходе которого специалисты пытаются проникнуть в корпоративную сеть через Интернет, и внутреннее, когда имитируются действия злоумышленника, имеющего физический доступ к сети компании. При проведении проверок специалисты применяют программные средства и приемы, используемые реальными злоумышленниками для взлома систем [2]. Тестирование проводится на сетевом, системном и прикладном уровне и позволяет выявить не только большинство уязвимостей, но и выделить среди них те, которые в комплексе позволяют реально скомпрометировать систему обеспечения информационной безопасности.

Самым трудоемким является анализ настроек безопасности информационных систем, который проводится с помощью специальных проверочных листов, содержащих описание конфигурации систем, рекомендованной профессионалами в области информационной безопасности. Основными достоинствами такого анализа являются высокая достоверность получаемой информации об имеющихся уязвимостях и минимальное влияние на работоспособность системы.

Наиболее эффективным является аудит, включающий в себя все виды аудиторских проверок, поскольку только он позволяет комплексно оценить защищенность компании перед лицом угроз информационной безопасности. Лучше всего, когда такой аудит проводится профессионально и независимо [3].

Для проведения аудита информационной безопасности предприятия привлекаются внешние компании, которые предоставляют консалтинговые услуги в области информационной безопасности, они выполняются группой экспертов, численность которых зависит от целей и задач обследования, а также от сложности объекта оценки [4].

При разработке плана для аудита необходимо учитывать принадлежность предприятия к критическим информационным инфраструктурам (КИИ), так как в этом случае нельзя говорить о неких одиночных «нарушителях», а необходимо рассматривать такие «кибервойска» как высокоразвитого и технически подготовленного злоумышленника, который с началом военных действий будет проводить непрерывные изощренные атаки в информационном пространстве [5]. Большинство руководителей предприятий не считают, что их объекты относятся к КИИ, это приводит к недостаточной защите данных, обрабатываемых в информационной системе предприятия [6].

Рассмотрим основные проблемы, возникшие в процессе проведения аудита, на примере ООО «Машиностроительный завод «РИВС»:

1. Отсутствие политики информационной безопасности, в которой описаны цели, план аудита и назначен специалист, ответственный за него.

2. Отсутствие поддержки и понимания высшего руководства компании в вопросах информационной безопасности и аудита, в частности.

3. Руководители головных предприятий не всегда готовы передавать филиалам документы, относящиеся к защите информации.

4. Отсутствие на предприятии специалиста по информационной безопасности. В большинстве организаций его задачи выполняются системными администраторами или специалистами других направлений, не осознающими специфики работы, рисков, и возможного ущерба [7].

Материалы были собраны при прохождении производственной практики на предприятии ООО «Машиностроительный завод «РИВС».

По данным сторонних компаний, отечественные автоматизированные системы управления технологическими процессами изначально создавались без расчета на внешнее вмешательство, таким образом, защитные механизмы таких систем оказались не приспособлены к отражению кибератак.

Только на основе проведенного аудита информационной безопасности, выявленных в процессе его проведения и своевременно устраненных недостатков, можно создавать эффективные и надежные системы информационной безопасности, в том числе и на объектах информатизации предприятий.

Литература

1. Mikhailova U.V., Barankova I.I., Lu'yanov G.I. Automated control system of a factory rail way transport based on ZIGBEE // 2016 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM) Proseedings. 2016.

2. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Прогнозирование локальных и внешних угроз на информационные серверы предприятия // Актуальные проблемы современной науки, техники и образования. 2017. Т. 1. С. 217-220.

3. Лихоносов А.Г., Денисов Д.В. Основы аудита информационной безопасности: учеб. пособие. Москва: МФПА, 2010.

4. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Подход к проектированию сети предприятия в защищенном исполнении // Вестник УрФО. Безопасность в информационной сфере. 2018. № 1 (27). С. 24-28.

5. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. DLP система: защита от утечки информации. Анализ поиска WORDSEARCH // Актуальные проблемы современной науки, техники и образования. 2016. Т. 1. № 1. С. 187-191

6. Михайлова У.В., Ершов В.А. Способы организации и методы противодействия DOS/DDOS – атакам // Безопасность информационного пространства: сборник трудов XIII Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных. Министерство образования и науки Российской Федерации, Южно-Уральский государственный университет, Кафедра «Безопасность информационных систем». 2015. С. 73-79.

7. Баранкова И.И., Михайлова У.В. Особенности формирования оценочных средств для сформированности компетенций специалиста по информационной безопасности // Информационное противодействие угрозам терроризма. 2015. Т. 2. № 25. С. 26-30.

References

1. Mikhailova U.V., Barankova I.I., Lu'yanov G.I. Automated control system of a factory rail way transport based on ZIGBEE // 2016 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM) Proseedings. 2016.

2. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I. Prognozirovaniye lokal'nykh i vneshnikh ugroz na informatsionnyye servery predpriyatiya // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. 2017. T. 1. S. 217-220.

3. Likhonosov A.G., Denisov D.V. Osnovy audita informatsionnoy bezopasnosti: ucheb. posobiye. Moskva: MFPA, 2010.

4. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I. Podkhod k proyektirovaniyu seti predpriyatiya v zashchishchennom ispolnenii // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. 2018. № 1 (27). S. 24-28.

5. Barankova I.I., Mikhaylova U.V., Luk'yanov G.I. DLP sistema: zashchita ot utechki informatsii. Analiz poiska WORDSEARCH // Aktual'nyye problemy sovremennoy nauki, tekhniki i obrazovaniya. 2016. T. 1. № 1. S. 187-191

6. Mikhaylova U.V., Yershov V.A. Sposoby organizatsii i metody protivodeystviya DOS/DDOS – atakam // Bezopasnost' informatsionnogo prostranstva: sbornik trudov XIII Vserossiyskoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchonykh. Ministerstvo obrazovaniya i nauki Rossiyskoy Federatsii, Yuzhno-Ural'skiy gosudarstvennyy universitet, Kafedra «Bezopasnost' informatsionnykh sistem». 2015. S. 73-79.

7. Barankova I.I., Mikhaylova U.V. Osobennosti formirovaniya otsenochnykh sredstv dlya sformirovannosti kompetentsiy spetsialista po informatsionnoy bezopasnosti // Informatsionnoye protivodeystviye ugrozam terrorizma. 2015. T. 2. № 25. S. 26-30.

БАРАНКОВА Инна Ильинична, доктор технических наук, заведующий кафедрой Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: Inna_Barankova@mail.ru

МИХАЙЛОВА Ульяна Владимировна, кандидат технических наук, доцент кафедры Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: ylianapost@gmail.com

БЫКОВА Татьяна Викторовна, студент кафедры Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г.И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: bykova.tatiana.mg@gmail.com

BARANKOVA Inna, Department, Nosov Magnitogorsk State Technical University (NMSTU), Doctor of Technical Sciences, Head of CSISE Department, Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: Inna_Barankova@mail.ru

MIKHAILOVA Uliana, Department, Nosov Magnitogorsk State Technical University (NMSTU), Ph.D.,Associate Professor of CSISE Department, Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: ylianapost@gmail.com

BYKOVA Tatyana, NMSTU, Student of CSISE Department, Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: bykova.tatiana.mg@gmail.com