УДК 004.056
DOI: 10.33764/2618-981X-2020-6-2-146-151

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ОПТИКО-ЭЛЕКТРОННОГО ПРИБОРОСТРОЕНИЯ

Муратжан Бактыярович Шакиров
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, 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 физики, тел. (903)937-27-90, e-mail: i.n.karmanov@ssga.ru

Автоматизированные системы играют ключевую роль в обеспечении бизнес-процессов коммерческих и государственных предприятий. Повсеместное использование автоматизированных информационных систем для хранения, обработки и передачи информации делает актуальными проблемы их защиты, особенно учитывая глобальную тенденцию к росту числа информационных атак, приводящих к значительным финансовым и материальным потерям. В статье продемонстрирована важность проведения аудита в сфере информационной безопасности оптико-электронного приборостроения. В статье рассмотрены этапы и правила проведения аудита информационной безопасности, а также критерии оценки результатов аудита. Аудит информационной безопасности – один из наиболее эффективных сегодня инструментов для получения независимой и объективной оценки текущего уровня защищенности предприятия от угроз информационной безопасности. Кроме того, результаты аудита дают основу для формирования стратегии развития системы обеспечения информационной безопасности организации.

Ключевые слова: аудит информационной безопасности, этапы проведения аудита, виды угроз, определение границ и глубины оценки, обследование информационных процессов, сбор и систематизация данных о видах информации.

INFORMATION SECURITY AUDIT OF AN OPTOELECTRONIC DEVICE ENGINEERING ENTERPRISE

Muratzhan B. Shakirov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, 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 the Department of Physics, phone: (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

Automated systems play a key role in supporting business processes of commercial and state enterprises. The widespread use of automated information systems for storing, processing and transmitting information makes the issues of their protection relevant, especially given the global trend towards an increase in the number of information attacks, leading to significant financial and material

losses. The article demonstrates the importance of conducting an audit in the field of information security of optoelectronic instrumentation. The article discusses the stages and rules of conducting an information security audit, as well as the criteria for evaluating its results. Information security audit is one of the most efficient tools for obtaining an independent and objective assessment of the current level of enterprise security from information security threats. In addition, the audit results provide the basis for forming a development strategy for the organization's information security system.

Key words: information security audit, stages and rules, types of threats, boundaries and depth of assessment, examining information processes, collecting and organizing data on types of information.

Введение

Сегодня информационные системы играют ключевую роль в обеспечении эффективности работы коммерческих и государственных предприятий. Повсеместное использование автоматизированных информационных систем для хранения, обработки и передачи информации делает актуальными проблемы их защиты, особенно учитывая глобальную тенденцию к росту числа информационных атак, приводящих к значительным финансовым и материальным потерям. Для эффективной защиты от атак компаниям необходима объективная оценка уровня безопасности информационных систем – именно для этих целей и применяется аудит безопасности.

Аудит безопасности информационных систем компании поможет защитить бизнес от потери данных. В данной статье описано, как провести процедуру и оценить результаты.

Что такое аудит информационной безопасности?

Существует несколько категорий угроз, способных привести к утечке, потере или ненадлежащему использованию информации в бизнесе. Первый вид – целенаправленные действия злоумышленников, намеревающихся получить доступ к данным и использовать их для получения выгоды. Способов много – от компьютерных атак и хищений до методов социальной инженерии и рейдерских захватов. Причем, атаки не обязательно совершают сторонние злоумышленники. Такими действиями вполне могут заниматься сотрудники компании: для шантажа, продажи, захвата власти и т.д. [1-3].

Второй источник – неосмотрительные действия, приводящие к уязвимостям в системе безопасности. Это может быть, например, использование сотрудниками зараженных программ или посещение инфицированных сайтов.

Третий вид угрозы – несоблюдение элементарных правил защиты: отсутствие антивирусов, беспорядочное хранение документов и беспрепятственный доступ к ним, отсутствие систем дублирования и т.д.

Особую опасность составляют несчастные случаи и стихийные бедствия – пожары, затопления, техногенные катастрофы, теракты и подобные им явления. Казалось бы, эта часть угроз имеет мало отношения к информации, но утерянные по этим причинам сведения и данные обычно ценнее, чем утрата имущества.

Наконец, одна из важных составляющих информационной безопасности, о которой иногда забывают, – отслеживание законодательных изменений и соблюдение норм российского права. Противопожарная защита и антивирусные программы не защитят от ареста и выемки данных по решению суда [4-5].

Аудит системы безопасности – комплекс мероприятий по выявлению и оценке этих угроз для конкретного бизнеса.

Этапы и правила проведения аудита информационной безопасности

Способ проведения аудита зависит от задач и уровня угрозы. Чем меньше компания и ниже продвинутость используемых технологий, тем меньше интерес злоумышленников и проще оценка. Важное условие перед началом аудита – составление технического задания на работающую систему информационной безопасности: и руководство компании, и аудитор должны представлять, как будет работать идеальная в их понимании служба [6-7].

Любой аудит состоит из обязательных этапов.

1. Определение границ и глубины оценки – на этом этапе руководство компании решает, в каких областях проводить обследование. Оптимальный вариант – сделать оценку по всем направлениям и максимально глубоко, но всегда возникает вопрос соответствия затрат и экономической эффективности применения полученных данных. Один из способов сокращения разного вида затрат – сужение зоны оценки до типовых блоков. Например, если в разных подразделениях используются схожие информационные системы, то высока вероятность, что в них присутствуют одинаковые уязвимости. Проверив полностью один филиал компании, остальные можно обследовать уже только на ошибки, обнаруженные в первом

2. Второй этап – сбор и систематизация данных о видах информации, которая возникает, хранится и передается внутри компании, и которой обмениваются с внешними контрагентами. На этом же этапе проводят инвентаризацию всех технических и программных средств, используемых для генерации, хранения и передачи данных.

3. Далее следует этап обследования информационных процессов. Здесь очень много подпунктов, и желательно не упустить ни один из них. Лучше всего, если человек, проводящий аудит, будет обследовать прохождение процессов прямо на рабочих местах, а не со слов исполнителей. В ходе этапа определяют участников информационных процессов, как проходят, какие ресурсы используют, требуемые согласования. По сути, процедура ничем не отличается от описания других бизнес-процессов в компании. Далее, основные пункты этого этапа, которые нужно проанализировать:

– как с информацией работает персонал;

– как происходит обучение сотрудников по обеспечению безопасности;

– кто и как управляет доступом к информации; понятие и документальное оформление тайны и конфиденциальной информации на предприятии;

– как обеспечивается защита от вредоносных программ;

– кто и как отслеживает события в сфере безопасности, как на них реагируют;

– алгоритмы шифрования данных, генерация, хранение и ликвидация паролей как происходит архивация, восстановление, дублирование данных;

– как используют мобильные, переносные, съемные устройства хранения данных;

– организация доступа в интернет и использования электронной почты в компании;

– как происходит доступ к информации для лиц, не являющихся сотрудниками;

– как контролируется доступ к сети внутри организации и извне.

4. Следующим шагом оценивают техническое и программное обеспечение: сетевое оборудование и компьютеры, базы данных, антивирусы и сетевые экраны, операционные системы на сервере и локальных машинах, средства интернет-коммуникации и другие пользовательские программы и приложения. Важно исследовать состояние не только виртуальных хранилищ, но и физических – архивные комнаты, сейфовое оборудование, в том числе, охранные и противопожарные сигнализации и средства.

5. На пятом этапе, когда создана целостная картина «как есть», ее сравнивают с тем, «как нужно», то есть с техническим заданием на структуру и функции безопасной информационной системы. В ходе этапа выявляют слабые места, ищут уязвимости и определяют риски.

6. Последний этап аудита – отчет для руководства (заказчика) с указанием недостатков и степени их опасности. Возможно составление плана первоочередных мероприятий по борьбе с высокорисковыми угрозами [7-10].

Как оценивать результаты аудита информационной безопасности

Ориентиром может быть международный стандарт ISO 17799, а также требованиям руководящих документов ФСТЭК (Гостехкомиссии) по управлению информационной безопасностью. Безусловно, для большинства предприятий внедрение всех его положений избыточно, но именно оттуда можно почерпнуть максимум знаний по этому вопросу [10].

Также важно, чтобы исполнитель, проводящий аудит, в отчете отразил приоритетность и степень каждой из угроз, чтобы руководитель представлял, в каком порядке и с какой скоростью следует приниматься за их устранение.

В общем случае аудит безопасности, вне зависимости от формы его проведения, состоит из четырех основных этапов, на каждом из которых выполняется определенный круг работ (рис. 1).

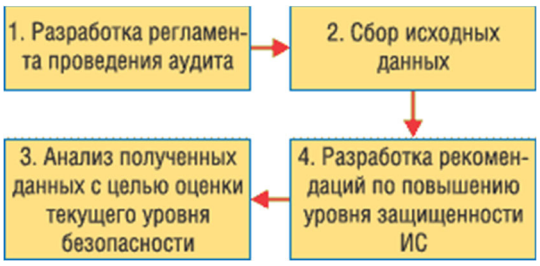

Рис. 1. Основные этапы работ при проведении аудита безопасности.

Результаты

Результатами аудита информационной безопасности являются:

1) описание и оценка текущего уровня защищенности информационной системы;

2) анализ рисков, связанных с возможностью осуществления внутренних и внешних угроз в отношении ресурсов информационной системы;

3) составление модели потенциального злоумышленника;

4) рекомендации по технической, организационной составляющей информационной безопасности (устранение уязвимостей в коде, разработка политики информационной безопасности);

5) получение максимальной отдачи от инвестиций, вкладываемых в системы защиты информации;

6) подтверждение того, что используемые внутренние средства контроля соответствуют задачам организации и позволяют обеспечить эффективность и непрерывность бизнеса;

7) обоснование инвестиций в системы защиты информации.

Заключение

Аудит информационной безопасности – один из наиболее эффективных сегодня инструментов для получения независимой и объективной оценки текущего уровня защищенности предприятия от угроз информационной безопасности. Кроме того, результаты аудита дают основу для формирования стратегии развития системы обеспечения информационной безопасности организации. Однако необходимо понимать, что аудит безопасности – не разовая процедура, он должен проводиться на регулярной основе. Только в этом случае аудит будет приносить реальную отдачу и способствовать повышению уровня информационной безопасности компании.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Аверченков, В. И. Аудит информационной безопасности [Текст]: учеб. пособие / В.И. Аверченков. – 3-е изд., стер. – М.: ФЛИНТА, 2016. – 269 с.

2. Барышева, О. С. Экономическая безопасность предприятий // Экономика и менеджмент инновационных технологий. 2017. № 1 [Электронный ресурс] – Режим доступа: http://ekonomika.snauka.ru/2017/01/13263 (дата обращения: 20.03.2020).

3. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. [Текст] – 8 с.

4. Дворникова, О. А., Макарова, Д. Г. Защита изделий двойного назначения при их разработке и эксплуатации в контексте ФЗ-187 [Текст] / Национальн. науч. конф. "Актуальные проблемы оптотехники": сб. материалов. – Новосибирск: СГУГиТ, 2018. – 91 с.

5. Демидов, Д. Е. Легкий, В. Н. Фисун, И. Д. Читава, А. Р. Интегрированный комплекс инженерно-технических средств охраны и системы контроля и управления доступом [Текст] // Интерэкспо ГЕО-Сибирь-2017. XIII Междунар. науч. конгр. : Национ. науч. конф. «Наука. Оборона. Безопасность-2017» : сб. материалов (Новосибирск, 17–21 апреля 2017 г.). – Новосибирск : СГУГиТ, 2017. – С. 7–12.

6. Menfis [Электронный ресурс] – Режим доступа: http://www.menfis-it.ru/uslugi/Admin1178467553.php. (дата обращения 25.03.2020).

7. Оюн, Ч. О., Попантонопуло, Е. В. Объекты критической информационной инфраструктуры [Текст] / // Интерэкспо ГЕО-Сибирь. XIV Междунар. науч. конгр. : Магистерская научная сессия «Первые шаги в науке» : сб. материалов (Новосибирск, 23–27 апреля 2018 г.). – Новосибирск : СГУГиТ, 2018. – С. 45–49.

8. Партыка, Т. Л. Информационная безопасность [Текст] / Партыка, Т. Л.. Попов, И. И – М.: Форум, Инфра-М, 2017**.** - 368 с.

9. Петухов, Р. Н. Обеспечение безопасности на промышленных предприятиях [Текст] / Молодой ученый. – 2016. – №1. – 458 с.

10. Якушенков, Ю. В. Основы оптико-электронного приборостроения [Текст] / Ю. В. Якушенков. – М.: Логос, 2013. – 376 с.