УДК 65.0
DOI: 10.33764/2618-981X-2021-6-230-234

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИЯХ В СОВРЕМЕННЫХ УСЛОВИЯХ

Кристина Анатольевна Николаева
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры информационной безопасности, тел. (913)715-96-47, e-mail: cristina.nikolaewa2016@yandex.ru

Аэлита Владимировна Шабурова
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доктор экономических наук, профессор, зав. кафедрой фотоники и приборостроения, директор института оптики и технологий информационной безопасности, тел. (383)344-40-58, e-mail: aelita_shaburova@mail.ru

На сегодняшний день актуальной проблемой является должное обеспечение информационной безопасности в организациях и предприятиях, поскольку доступ к защищенной информации может нанести значительный ущерб компании и её финансовому положению. Исходя из того, что наибольшее внимание и защита требуются информации на предприятиях, в данной статье рассмотрены различного рода причины нарушения информационной безопасности, а также средства и методы защиты этой информации. Потребность в защите информации обуславливается увеличением её значимости за последние годы, тем самым объясняется актуальность данной статьи.

Ключевые слова: техническое обеспечение, информационная безопасность, система информационной безопасности, организационное обеспечение

THE PROBLEM OF ENSURING INFORMATION SECURITY AT ENTERPRISES IN MODERN CONDITIONS

Kristina A. Nikolaeva
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Information Security, phone: (913)715-96-47, e-mail: cristina.nikolaewa2016@yandex.ru

Aelita V. Shaburova
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, D. Sc., Professor, Head of Department of Photonics and Device Engineering, Director, Institute of Optics and Information Security Technologies, phone: (383)344-40-58, e-mail: aelita_shaburova@mail.ru

Today, an urgent problem is the proper provision of information security in organizations and enterprises, since access to protected information can cause significant damage to the company and its financial position. Based on the fact that the greatest attention and protection is required for information in enterprises, this article will consider, of various kinds, the causes of information security violations, as well as the means and methods of protecting this information. The need to protect information is caused by the increase in its importance in recent years, which explains the relevance of this article.

Keywords: technical support, information security, information security system, organizational support

Введение

В настоящее время неотъемлемой частью функционирования всех действующих организаций является информационная безопасность (ИБ) этих организаций. Основными составляющими ИБ считается конфиденциальность информации, целостность и доступность.

Сегодня рост нарушений ИБ и негативных последствий от них очень велик, что обуславливает обострение проблем ИБ в условиях интенсивного совершенствования технологий и средств защиты данных. Сама система защиты информации заключается в мониторинге угроз, ликвидации источников угроз, их предотвращении, а также, негативных последствий от них.

Обеспечение ИБ в наше время является многогранной проблемой, поскольку защита информации необходима для всех носителей информации – организаций, предприятий, государства и общества.

Проблемы обеспечения информационной безопасности на предприятиях

Одной из основополагающих проблем защиты информации является некорректное моделирование угроз. Некорректное рассмотрение факторов всегда усугубляется реализацией угроз безопасности, которые значимое влияние имеют в финансово-экономических показателях деятельности и работоспособности организации вплоть до прекращения его функционирования.

Важным моментом корректного моделирования угроз безопасности является необходимость определения списка актуальных угроз и потенциальных нарушителей, чтобы избежать ненужных затрат и исключить возможность потери конфиденциальной информации.

Система информационной безопасности (СИБ) является совокупностью защитных мер, средств защиты и рабочих процессов, включая ресурсную и административную (организационную) поддержку.

Не менее важной проблемой является то, что руководитель предприятия не всегда имеет достаточный уровень осведомленности о степени важности СИБ и не готов выделять ресурсы как на содержание сотрудника, ответственного за поддержание ИБ, так и для своевременного повышения квалификации имеющихся сотрудников отдела ИБ.

Однако и в техническом обеспечении имеется ряд определенных проблем. Техническое обеспечение – это комплекс технических мероприятий, обеспечивающих работу системы защиты информации. Эти технические меры включают в себя: системы регистрации событий, анализа информационной безопасности, системы контроля и мониторинга информационной безопасности, системы предотвращения утечек информации, системы защиты от воздействия вредоносного кода, системы контроля подключения и использования съемных носителей, системы контроля доступа и т.д.

В этом комплексе одной из проблем является недостаточный уровень профессионализма сотрудника, ответственного за обеспечение ИБ при установке,

настройке, эксплуатации и мониторинге работоспособности технических средств защиты информации, что может привести к уязвимостям, которые, в свою очередь, могут быть использованы нарушителями для реализации угроз информационной безопасности предприятия.

Кроме того, руководители предприятий не готовы выделять средства на приобретение готовых технических решений для защиты информации и Digital Light Processing-систем (DLP-систем). Так же не готовы определять полномочия и права сотрудников, ответственных за обеспечение ИБ, и в целом для того, чтобы контролировать эту область, они не способны учитывать мнения и замечания таких сотрудников, которые не приносят для организации прибыль, а только лишь постоянно требуют выделения денежных средств на приобретение средств защиты информации.

Еще одной проблемой может являться приобретение недорогих готовых продуктов и решений, которые не прошли установленные процедуры сертификации уполномоченных лиц, не соответствуют требуемым характеристикам для таких систем и не входят в поставляемый пакет технической поддержки. Неспособность улучшить существующие системы может снизить качество их функционирования и степень надежности таких систем.

Возможные решения проблем в обеспечении информационной безопасности на предприятиях

В настоящие время одним из наиболее актуальных способов решения проблем информационной безопасности на предприятиях является организационное обеспечение, которое предусматривает установление на предприятии временных, территориальных, пространственных, правовых, методических и иных ограничений. Ограничения устанавливаются действующими качественными комплексными внутренними нормативными документами, инструкциями, положениями, приказами.

Такие документы в обязательном порядке должны содержать:

– индивидуальную ответственность сотрудников;

– последствия за разглашение конфиденциальной информации;

– применение санкций за несоблюдение требований нормативных документов;

– безопасность работы в определенных информационных системах и ее порядок;

– установлен запрет на определенные действия;

– порядок действий в различных ситуациях;

– список лиц, ответственных за поддержание обеспечения информационной безопасности, их полномочия, а также выделяемые ресурсы.

В тех случаях, когда руководство предприятия некомпетентно и безответственно относиться к вопросам обеспечения должного уровня информационной безопасности и не готово выделять необходимые ресурсы, сотруднику, ответственному за обеспечение ИБ, необходимо донести руководителю информацию о необходимости предоставления полномочий и финансирования. Для того, чтобы быть убедительным, руководителю предприятия нужно предоставить

оценку рисков и возможных последствий в виде доводов и обоснований. В этом случае многое зависит от настойчивости, коммуникабельности и компетентности сотрудника отдела ИБ.

При должном уровне осознания руководством значимости информационной безопасности, грамотном расчете потенциальных рисков, своевременном совершенствовании имеющихся систем, а также при должном финансировании большинство проблем, связанных с нарушением ИБ, и как следствие, с финансовыми потерями и потерей деловой репутации, можно избежать.

Заключение

На сегодняшнее время главной проблемой информационной безопасности на предприятиях является отсутствие продуманной утвержденной политики обеспечения ИБ, а также не совсем верное понимание концепции ИБ предприятия в целом. Все действующие организации в настоящий момент предпринимают необходимые меры по защите информации, однако эти меры применимы только для устранения отдельных угроз, что влечет за собой большое количество уязвимостей, создавая предпосылки для дальнейшего негативного воздействия.

Для полного осуществления защиты информации на предприятиях большинству организациям нужен систематизированный подход абсолютно во всем: в изложении целей, задач и детального набора мер, направленных на защиту информации. Иными словами, необходима некая концепция ИБ, задача которой будет заключаться в следующем:

1) в защите организаций от различного рода источников угроз, вызванных различными действиями, связанными с информационными ресурсами;

2) в реализации защиты существующей информационной инфраструктуры предприятия;

3) в обеспечении таких условий, которые создают все предпосылки для локализации любого ущерба;

4) в оперативном мониторинге и выявлении всевозможных угроз;

5) в непрерывном контроле действующей системы защиты;

Делая вывод, можно с уверенностью заявить, что актуальная проблема защиты информации на предприятиях является следствием отсутствия комплексной защиты информации, которая подразумевает системный характер, реализация которой обеспечит определенную основу для развития системы информационной безопасности для различных организаций и в тоже время ограничит возможность влияния на них нового источника угроз.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Балановская А.В. Обеспечение информационной безопасности предприятий промышленности [Текст] / А.В. Балановская // Вестн. Самр. Гос. ун-та. – Самара, 2011. – С. 72-79.

2. Васильков А.В. Информационные системы и их безопасность [Текст] учеб. пособие / А.В. Васильков, А.А. Васильков, И.А. Васильков. – М.: Форум, 2011. – С. 528.

3. Голенищев Э.П. Информационное обеспечение систем управления [Текст] учебник/ Э.П. Голенищев, И.В. Клименко. – Ростов на Дону: Феникс, 2010. – С. 320.

4. Гришина Н.В. Комплексная система защиты информации на предприятии [Текст] учеб. пособие / Н.В. Гришина – М.:Форум, 2010. – С. 240.

5. Дорофеев А.В. Безопасный удаленный доступ к корпоративным ресурсам: Существующие концепции и решения [Текст] / А.В. Дорофеев // Connect! Мир связи. 2010. – С. 34-38.

6. Мельников В.П. Информационное обеспечение систем управления [Текст] учебник / В.П. Мельников. – М.: Академия, 2010. С. 336.

7. Сердюк В.А. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Текст] учеб. пособие / В.А. Сердюк. – М.: Высшая шк. экономики, 2011. – С. 576.

8. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». [Текст]. Нац. стандарт. РФ 2016.

9. Чипига А.Ф. Информационная безопасность автоматизированных систем [Текст] / А.Ф. Чипига – М.: Гелиос АРВ. 2010. – С. 336.

10. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей [Текст] / В.Ф. Шаньгин – М.: Инфра-М, 2011. - С. 416.