УДК 621.311

К ВОПРОСУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ПРЕДПРИЯТИЙ

Ложкова Ю.Н.,

кандидат технических наук,

доцент кафедры экономики предпринимательства,

Бийский технологический институт (филиал) ФГБОУ ВО АлтГТУ,

Российская федерация, г. Бийск

Аннотация: В работе раскрыто понятие информационной безопасности организаций, выявлены основные угрозы нарушения целостности информации, представлена общая структура системы информационной безопасности, а также предложены основные направления действий по повышению уровня защиты информации о деятельности предприятий.

Ключевые слова: цифровая экономика, конфиденциальная информация, защита данных, информационная безопасность, угрозы информационной безопасности.

TO THE QUESTION OF INFORMATION SECURITY OF MODERN ENTERPRISES

Lozhkova Yu.N.,

Candidate of Technical Sciences, Associate Professor,

Biysk Technological Institute (branch) of the Altay State Technical University,

Biysk, Russia

Annotation: The paper reveals the concept of information security of organizations, identifies the main threats to the violation of the integrity of information, presents the general structure of the information security system, and proposes the main areas of action to improve the level of protection of information about the activities of enterprises.
Keywords: confidential information, data protection, information security, information security threats.

В аспекте развития цифровой экономики в нашем государстве, основными ресурсами которой являются данные, знания и информация, особенно актуальным становится вопрос информационной безопасности предприятий.

Под информационной безопасностью понимается защищённость информации и поддерживающей инфраструктуры. Пара строк с описанием нового продукта могут стоить предприятию миллионы рублей. Обеспечить информационную безопасность – значить не дать, чтобы эта «пара строк» ушла в руки злоумышленника. Поэтому, прежде чем переходить к рассмотрению вопроса информационной безопасности, необходимо определиться с терминологическим аппаратом исследования. Начнем с понятия, что такое информация, и как её можно и нужно защищать [1, с.17-19].

В открытых источниках под информацией разные авторы понимают сведения независимо от формы их представления; знания о предметах, фактах, идеях и т. д., которыми могут обмениваться люди в рамках конкретного контекста (ISO/IEC 10746-2:1996); сведения, воспринимаемые человеком и (или) специальными устройствами как отражение фактов материального или духовного мира в процессе коммуникации (ГОСТ 7.0-99) и т. д.

Если обращаться к специфике работы предприятий и организаций, то информация может представлять собой, например, переговоры начальников в

«курилке», письма, приходящие и отсылаемые с корпоративных ящиков ежедневно сотнями и тысячами, технические задания изделий, служебная документация, особенности организации и работы организации. Таким образом, это то, что выбрасывается в мусорные вёдра и забывается на столах у коллег.

Но далеко не все сведения имеют важность, а, значит, прежде чем перейти к защите, нужно понять, что защищать, а что нет.

Сведения, распространение или уничтожение которых нанесёт ощутимый вред предприятию, называются активами. Всего у активов выделяют три основных свойства:

– конфиденциальность;
– целостность;
– доступность.

Под конфиденциальностью понимается, что актив недоступен лицам без соответствующего доступа. Доступность означает, что сведения используется только сотрудниками, имеющими на это право. Целостность – это неповреждённость сведений. Таким образом, задача информационной безопасности сводится к обеспечению этих трёх свойств. Следующий этап после определения активов, которые требуется защищать – изучение угроз [2, с. 77].

Угроза – это некоторые действия или события, в результате которых активам организации будет нанесён ущерб. Примеры угроз:

– «слив» критически важной информации конкурентам;
– внезапная смерть или уход специалиста, без которого проект нереализуем;
– падение метеорита или другое чрезвычайное или непредсказуемое происшествие;

– взлом компьютерной сети.

Если компьютерная сеть предприятия будет взломана, злоумышленник получит доступ к информации и нанесёт этим вред. При падении метеорита предприятие перестанет существовать. По убыткам второе событие во много раз превышает первое, но организации не переезжают в подземные бункеры, а ставит антивирусы. Причина – в разнице вероятностей реализации этих двух угроз.

Действительно, вероятность падения метеорита на здание мала. И постройка подземного бункера обойдётся в сотни раз дороже, чем аренда или покупка офисного здания. Между тем, в мире часто проводятся кибернетические атаки, и в свете последних событий – массового заражения вирусом «Wanna Cry» – приобретение средств защиты информации имеет смысл.

На любом предприятии реализован некоторый уровень информационной безопасности. Другой вопрос, насколько этот уровень высок. Для понимания этого, необходимо ответить на следующие вопросы:

– Работают ли сотрудники на компьютерах, защищённых паролями?

– Блокируют ли компьютеры, отходя от рабочего места?

– Легко ли постороннему человеку пройти на территорию организации?

– На эти и другие вопросы отвечает аудит информационной безопасности.

Аудит информационной безопасности

Безусловно, необходимость достижения безопасности информации не требует доказательств. Информацию о защищённости предприятия получают, проводя аудит в следующих направлениях:

– аттестация всего, связанного с информацией и поддерживающей инфраструктурой;

– контроль защищённости информации;

– исследования устройств на наличие побочных электромагнитных излучений и наводок;

– проектирование с учётом необходимости соответствия требованиям информационной безопасности.

Аттестация, как правило, проводится сторонними организациями. Цель аттестации – выявить, соответствует ли объект предъявляемым требованиям безопасности. При аттестации могут быть выявлены уязвимости – особенности автоматизированных систем, систем связи, технических средств и тому подобных объектов, которые могут быть использованы злоумышленником [3, с. 145-146].

Под контролем защищённости понимается изучение способов доступа к информационным ресурсам, а также наблюдение за эффективностью средств, обеспечивающих защиту этого ресурса. Примеры способов доступа:

– прослушивание помещений с помощью «жучков»;

– кража пароля с целью получения доступа к компьютеру сотрудника;

– изучение мусорной корзины;

– отсылка письма с трояном сотруднику, чтобы получить удалённый доступ к корпоративной сети;

– расспросы сотрудников с целью выведать конфиденциальную информацию.

Использование этих путей получения информации в корыстных целях – потенциальная угроза. Поэтому необходимо наблюдать за ними, а также за работой системы защиты информации, которая предотвращает реализацию этих угроз.

С помощью анализа и обработки побочных излучений можно получить информацию конфиденциального характера. К примеру, использование

телефонов, переговорных устройств порождает электромагнитные излучения. Эти излучения можно преобразовать в акустическую информацию. Затем и проводится аудит устройства на наличие таких излучений и подводок.

Некоторые помещения требуют повышенного уровня безопасности. Например, залы для переговоров, кабинеты высшего руководства. В таких помещениях важно учитывать расположение окон, дверей, силовых кабелей, розеток, толщина и исполнение стен.

Безопасно проектировать можно и автоматизированные системы: каким образом будут использоваться её составляющие, какие данные будут подаваться на вход и так далее. Безопасное проектирование – также важное направление аудита безопасности.

Различают внешний и внутренний аудит. И если внешний аудит проходит разово, желательно на регулярной основе, то внутренний проводится постоянно с целью актуализации информационной безопасности. При проведении аудита следует руководствоваться политикой безопасности, регламентирующей в общих чертах что защищать и как. Речь об этом документе пойдёт в следующем разделе.

Политика информационной безопасности предприятия

Выше были подробно рассмотрены основные активы, угрозы и уязвимости информационной безопасности предприятий. Еще одними из важных факторов в данном направлении являются риски и оценка рисков. Дело в том, что каждый актив имеет свою стоимость, а атака на актив – свои последствия.

Под угрозой понимается атака или событие (к примеру, природное явление), которое приносит ущерб активу. Но угрозе не совершиться, если нет уязвимости – особенности в защите предприятия, которую можно использовать ему во вред.

Риск – это вероятность совершения угрозы через существующую уязвимость, помноженная на сумму, в которую оценивается ущерб, нанесённый активу. Чем выше вероятность и выше стоимость, тем выше риск, и наоборот. Некоторые риски с высокой стоимостью ущерба, как падение метеорита, будут низкими из-за очень малой вероятности осуществления.

Поэтому в политике информационной безопасности не встретить ответственного за действия при падении метеорита лица – и при этом часто можно увидеть ответственного при кибернетической атаке.

Таким образом, политика информационной безопасности предприятия – это документ, в котором:

– определяются основные термины безопасности, например «информационная безопасность», «защита информации»;

– прописываются основные риски и ситуации, возникающие при реализации рисков;

– определяются общие требования для предотвращения реализации рисков, детектирования, реагирования и восстановления в случае, если риск всё-таки осуществится.

В политике безопасности можно встретить список действий при приёме сотрудника на работу, описание контрольно-пропускной системы, требования, предъявляемые при работе с автоматизированными системами, и другие жизненно важные моменты. Именно этот документ используется в первую очередь при организации защиты информации.

Защита информационной безопасности

Следует разделять организационные и технические меры защиты. Ведь организация состоит в первую очередь из сотрудников, и только потом из зданий, мебели, компьютеров и другого имущества. Потому важная часть безопасности – это проведение семинаров, составление брошюр о защите собственных данных от утечки.

Кроме того, необходима постоянная мотивация сотрудников, обеспечение им комфортных условий, а также наличие штрафных мер – важно балансировать между «кнутом и пряником», чтобы не получить в результате сотрудника-злоумышленника.

Регулярное проведение аудитов и актуализация политики безопасности также входит в организационные меры. Необходимо доводить до сотрудников изменения в политике для поддержания уровня защищённости. Уязвимости, выявленные при аудите технических средств, должны учитываться и при необходимости закрываться.

Под техническими методами понимается защита от несанкционированного доступа к информации. Среди технических методов распространены: видеонаблюдение; контроль и разграничение прав доступа; контроль доступа к информационным ресурсам; использование парольной защиты; установка средств защиты информации; блокирование, зашумление наводок и излучений.

Средства защиты информации позволяют контролировать корпоративную среду и быстро реагировать на события, отвечающие признакам реализации угрозы. Контрольно-пропускная система исключит возможность появления стороннего нарушителя, а система видеонаблюдения позволит среагировать или выяснить, если сотрудник делает то, что не должен делать, или находится там, где не должен быть.

Контроль доступа к информационным ресурсам не даст сотруднику безосновательно получить важные сведения, а блокировка излучений усложнит удалённое считывание информации.

Существуют комплексные средства защиты информации, при установке которых организация может быть уверена, что она защищена со всех сторон. Но иногда достаточно установить качественный антивирус со встроенным

межсетевым экраном, прочитать лекцию сотрудникам, нанять вахтёра и тем самым закрыть актуальные угрозы, не потратившись на излишний функционал.

Благодаря аудиту и политике информационной безопасности предприятие точно будет знать, что и как необходимо защитить, а, значит, организует безопасность по принципу разумной достаточности, что в конечном итоге способно положительно отразиться на показателях его финансово-хозяйственной деятельности.

Библиографический список

1. Ложкова, Ю.Н. Информационный менеджмент: учебное пособие для бакалавров по направлению обучения 38.03.05 «Бизнес-информатика» / Ю.Н. Ложкова; Алт. гос. техн. ун-т, БТИ. – Бийск: Изд-во Алт. гос. техн. ун-та, 2016. – 139 с.

2. Рахимова Г. А. Информационная безопасность для бизнес-организаций // Молодой ученый. – 2016. – № 9. – С. 77-79.

3. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. – 702 с.

Оригинальность 95%