ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОРГАНИЗАЦИИ

О.М. Васильева, *магистрант МТУСИ, 111024, г. Москва, ул. Авиамоторная, 8А., o.vasileva2015@yandex.com;*
Р.С. Хлебников, *магистрант МТУСИ, 111024, г. Москва, ул. Авиамоторная, 8А., Romankhleb@yandex.ru*

УДК 004.056

Аннотация. Рассмотрена роль информационной безопасности в организации, показаны составляющие элементы и мероприятия, входящие в данное понятие. Дано определение защиты информации на предприятии. Перечислены базовые принципы безопасности информации. Отражены основные методы защиты информации, а также средства, необходимые для реализации данных методов.

Ключевые слова: информационная безопасность в организации; защита информации; система физической защиты; аппаратные средства защиты; программные средства защиты.

INFORMATION SECURITY IN THE ORGANIZATION

Olga Vasileva, *graduate student MTUCI*
Roman Khlebnikov, *graduate student MTUCI*

Annotation. The role of information security in the organization is considered; the constituent elements and activities included in this concept are shown. The definition of information security in the enterprise is given. The basic principles of information security are listed. Reflects the main methods of protecting information, as well as the means necessary to implement these methods.

Keywords: information security in an organization; protection of information; physical protection system; hardware protection; software protection.

Мировой прогресс в информационном обеспечении ставит новые задачи не только перед государствами, но и субъектами экономики страны в защите своего информационного пространства от несанкционированного доступа. Усиливается роль служб информационного обеспечения организации, проводятся работы по анализу уязвимости каналов связи. Все эти явления обуславливают актуальность информационной безопасности в организации.

Целью исследования выступает определение роли информационной безопасности в организации. Задачи проведенного нами исследования:

1. Выявить мероприятия, необходимые для обеспечения информационной безопасности.
2. Выяснить – на каких принципах должна базироваться система информационной безопасности на предприятии.
3. Рассмотреть методы минимизации угроз информационной безопасности организации.

Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода [1].

Безопасность информации – состояние защищенности данных, при которых обеспечены их доступность, конфиденциальность и целостность [2].

Информационная безопасность организации, по нашему мнению, должна включать следующие мероприятия:

1. Анализ потенциальных внешних и внутренних угроз.

2. Оценка уязвимости и защиты информации.
3. Создание дорожной карты мер предотвращения угроз.
4. Выполнение задач по ликвидации угроз.

Главная роль обеспечения защиты данных на предприятии – это создать необходимые условия для бесперебойной работы информационной системы и предотвращение возможных атак на нее.

Защита информации включает полный комплекс мер по обеспечению целостности и конфиденциальности информации при условии ее доступности для пользователей, имеющих соответствующие права.

Целостность – понятие, определяющее сохранность качества информации и ее свойств.

Конфиденциальность предполагает обеспечение секретности данных и доступа к определенной информации отдельным пользователям.

Доступность – качество информации, определяющее ее быстрое и точное нахождение конкретными пользователями [2].

Безопасность информации на предприятии основывается на пяти принципах:

1. Принцип системности. Защитные меры организации должны быть направлены на предотвращение информационной атаки как со стороны внешних нарушителей, так и со стороны внутренних. При этом необходимо учитывать каналы закрытого доступа, применяемые средства защиты.

Применение средств защиты должно совпадать с вероятными видами угроз и функционировать как комплексная система защиты, технически дополняя друг друга. Комплексные методы и средства обеспечения информационной безопасности организации являются сложной системой взаимосвязанных между собой процессов.

2. Принцип многоуровневой защиты направлен на создание рубежей защиты информационной системы, состоящих из последовательно расположенных зон безопасности, главная из которых будет находиться внутри всей системы.

3. Принцип прочности. Правила обеспечения информационной безопасности в организации должны охватывать весь спектр зон безопасности. Все они должны быть иметь одинаковую степень надежной защиты с определением возможной угрозы.

4. Принцип благоразумности представляет собой разумное применение защитных мер с необходимой степенью безопасности. Данный принцип обусловлен целесообразностью огромных материальных затрат и дальнейшей рациональности их использования. Себестоимость мер защиты не должна быть больше размера вероятного ущерба, а также расходы на работоспособность и обслуживание защитной системы.

5. Принцип бесперебойности. Функционирование информационной безопасности должна быть непрерывной и бесперебойной.

С целью минимизации угроз информационной безопасности организации используются следующие методы:

1. Препятствие. Метод представляет собой использование физической силы с целью защиты информации от преступных действий злоумышленников с помощью запрета на доступ к информационным носителям и аппаратуре.

2. Управление доступом – метод, который основан на использовании регулирующих ресурсов автоматизированной системы, предотвращающих доступ к информационным носителям. Управление доступом осуществляется с помощью таких функций, как:

- идентификация личности пользователя, работающего персонала и систем информационных ресурсов такими мерами, как присвоение каждому пользователю и объекту личного идентификатора;

- аутентификация, которая устанавливает принадлежность субъекта или объекта к заявленному им идентификатору;
- проверка соответствия полномочий, которая заключается в установлении точного времени суток, дня недели и ресурсов для проведения запланированных регламентом процедур;
- доступ для проведения работ установленных регламентом и создание необходимых условий для их проведения;
- регистрация в виде письменного протоколирования обращений к доступу защитных ресурсов;
- реагирование на попытку несанкционированных действий в виде шумовой сигнализации, отключения, отказа в запросе и в задержке работ.

3. Маскировка – метод криптографического закрытия, защищающий доступ к информации в автоматизированной системе.

4. Регламентация – метод информационной защиты, при котором доступ к хранению и передаче данных при несанкционированном запросе сводится к минимуму.

5. Принуждение – это метод, который вынуждает пользователей при доступе к закрытой информации соблюдать определенные правила. Нарушение установленного протокола приводит к штрафным санкциям, административной и уголовной ответственности.

6. Побуждение – метод, который основан на этических и моральных нормах, накладывающих запрет на использование запрещенной информации, и побуждает соблюдать установленные правила [3].

Все перечисленные методы защиты основаны на следующих средствах:

1. Система физической защиты (СФЗ). Применяется в качестве внешнего контроля за месторасположением объекта и защиты информационной системы в виде специальных устройств. Рассмотрим основные элементы СФЗ (табл. 1).

Таблица 1

№	Элемент СФЗ	Характеристика
1.	Глубоко эшелонированная защита	Направлена на создание многоуровневой системы преград для внешнего нарушителя
2.	Система видеонаблюдения	С помощью данной системы распознается нарушитель
3.	Система контроля доступа к объектам	Автоматизированная информационная система, позволяющая определить лицо, имеющее доступ к объектам

Как видно из табл. 1, основными элементами СФЗ являются глубоко эшелонированная защита в виде автоматизированной системы ограждения, систем видеонаблюдения и система контроля доступа к объектам. Все эти элементы СФЗ должны находится на постоянном контроле согласно утвержденному порядку в организации.

2. Аппаратные средства защиты представлены электронными и автоматизированными механическим устройствам. Они встроены в блоки автоматизированной информационной системы, представляющие собой самостоятельные устройства, соединенные с данными блоками.

Основная их функция – это обеспечение внутренней защиты соединительных элементов и систем в вычислительной технике – периферийного оборудования, терминалов, линий связи, процессоров и других устройств.

Обеспечение безопасности информации с помощью аппаратных средств включает:

1) Обеспечение запрета неавторизированного доступа удаленных пользователей и АИС (автоматизированная информационная система);
2) Обеспечение надежной защиты файловых систем архивов и баз данных при отключениях или некорректной работе АИС;
3) Обеспечение защиты программ и приложений.

Вышеперечисленные задачи обеспечения безопасности информации обеспечивают аппаратные средства и технологии контроля доступа (идентификация, регистрация, определение полномочий пользователя).

Обеспечение безопасности особо важной информации может осуществляться с использованием уникальных носителей с особыми свойствами, которые предотвращают считывание данных.

Программные средства защиты входят в состав ПО (программного обеспечения), АИС или являются элементами аппаратных систем защиты. Такие средства осуществляют обеспечение безопасности информации путем реализации логических и интеллектуальных защитных функций и относятся к наиболее популярным инструментам защиты. Это объясняется их доступной ценой, универсальностью, простотой внедрения и возможностью доработки под конкретную организацию или отдельного пользователя. В то же время, обеспечение безопасности информации с помощью ПО является наиболее уязвимым местом АИС организаций.

Таким образом, используя максимально различные способы защиты, служба информационной безопасности создает такую систему информационной безопасности, которая позволяет сохранить информационные данные, снизить до минимума риски несанкционированного доступа к различного рода сведениям, имеющим важное значение для функционирования организации.

Литература

1. Храмогин, П.А. Принципы информационной безопасности // Молодежь и наука: сборник материалов X Юбилейной Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых с международным участием, посвященной 80-летию образования Красноярского края [Электронный ресурс]. Красноярск: Сибирский федеральный ун-т, 2014. Режим доступа: http://conf.sfu-kras.ru/sites/mn2014/directions.html, свободный. с международным участием, посвященной 80-летию образования Красноярского края
2. Грошева Е.К., Невмержицкий П. И., 2017 Информационная безопасность: современные реалии // Бизнес-образование в экономике знаний, 2017. – № 3. – С. 36.
3. URL http://www.iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti/ (дата обращения – октябрь 2018 г.).