ОСОБЕННОСТИ ПРОЦЕССА АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННЫХ СИСТЕМ

А.В. Моргунов, Я.И. Борцова
Алтайский государственный университет, г. Барнаул

Сегодня весьма актуальной является быстрорастущая зависимость бизнес-процессов от информационных систем, заставляющая уделять все больше внимания вопросам информационной безопасности и тем самым создавая тенденцию на внедрение цифровых технологий во всех направлениях деятельности. Правильно выстроенная система защиты информации исключает возникновение инцидентов, в результате, которых будет нанесён вред финансовому комплексу предприятия, а также возможность негативно повлиять на имидж компании в целом. Следовательно, массовое внедрение и применение различных цифровых технологий приведёт к созданию полноценных условий для осуществления продуктивного рабочего процесса как отдельных подразделений, так и предприятия в целом.

Сбалансированная и грамотная работа сотрудников, надёжность техники, правильная организация всех процессов и систем является гарантом осуществления высокоэффективного рабочего процесса, а значит и получения в итоге высоких результатов. Основным условием практической реализации такой структуры является надёжная и постоянно совершенствующаяся, согласно требованиям времени, система обеспечения безопасности. Для полноценного осуществления своей деятельности необходимо обеспечить соответствие всех необходимых ресурсов, процессов, объектов, установленным законами стандартам.

Главным инструментом реализации эффективной деятельности такого типа предприятий, как в мировой, так и в российской практике, является аттестация объектов и информационных систем. Подробное изучение особенностей процесса аттестации является залогом успешного прохождения всех необходимых испытаний. Данный процесс в полной мере обеспечит безопасное функционирование всех информационных ресурсов и создаст рабочие условия, исключающие получение несанкционированного доступа или же разглашение конфиденциальной информации.

Актуальность данной работы заключается в том, что сегодня далеко не все предприятия после прохождения аттестационных мероприятий продолжают соблюдать установленные регламентом и

законом требования безопасности, тем самым создавая уязвимость для внешних и внутренних атак. Также огромную опасность представляет повышенный уровень совершения киберпреступлений. Чаще всего мошенниками используются уязвимости в информационных сетях, создаваемые в ходе рабочего процесса рядовыми пользователями данной сети по причине несоблюдения установленных требований.

В рамках развития стратегии по снижению и исключению рисков в области защиты передачи информации, объектами информатизации постоянно разрабатываются и внедряются современные технологии, направленные на обнаружение отклонений от базового состояния защиты информационных ресурсов, а также комплекс мероприятий для принятия оперативных, и в случае необходимости корректирующих мер, в режиме круглосуточной работы. Основными направлениями данной работы являются:

1. Контроль антивирусной защиты;
2. Контроль защиты сетевой и прикладной инфраструктуры;
3. Контроль криптографической защиты информации;
4. Отслеживание корреляций событий информационной безопасности и предотвращение вторжений;
5. Сопровождение информационной безопасности нормативно-методологической базой;
6. Контролируемый доступ к информационным ресурсам с помощью автоматизированной системы, включающей пользователей с особыми учётными записями, обеспечивающими контроль доступа.

Нарушение или невыполнение хотя бы одного из вышеперечисленных пунктов может привести как к финансовому, так и информационному ущербу объекта информатизации, что негативно скажется на развитии и деятельности предприятия в целом. Аттестация, как индикатор, выявляет слабые места в производственных процессах предприятия, тем самым дает направления по устранению недостатков, усовершенствованию, имеющихся технологий и разработке новых, с учетом исключения допущенных ошибок и как следствие обеспечивает защиту от финансовых рисков.

Рассмотрим особенности проведения аттестации объекта информатизации. В Российской Федерации аттестация является обязательной составляющей осуществления рабочего процесса предприятия, которое:

1. Обладает государственной тайной;

2. Осуществляет засекреченные переговоры по специальным линиям связи;
3. Осуществляет защиту информационных ресурсов государства;
4. Управляет экологически опасными объектами;

Аттестационный процесс сводится к проведению комплексной проверки (испытаний) объекта или системы в реальных условиях, целью которых будет инспектирование соответствия используемых средств и ресурсов установленному уровню безопасности. Основными категориями экспертизы чаще всего выступают:

1. Охрана информации от несанкционированного доступа;
2. Предотвращение утечки информации посредством побочных электромагнитных излучений;
3. Охрана информации от стороннего воздействия с помощью специализированных устройств, находящихся в объекте или системе информатизации.

Процесс аттестации осуществляется особыми органами, выбирающими определённые параметры аттестации для каждого информационного объекта в отдельности, в зависимости от специфики деятельности объекта информатизации. Однако, в общем случае данный перечень состоит из:

1. Предварительного знакомства с объектом и сбора необходимых о нём сведений;
2. Подробного анализа полученных данных;
3. Проведения экспертизы объекта (системы) и проверки разработанной документации по защите информации на соблюдение требований, установленных в этой документации;
4. Проведения различных испытаний с помощью специальной контрольной аппаратуры и тестирующих устройств;
5. Проведения исследования программно-технических элементов в специализированных центрах, занимающихся сертификацией средств защиты информации;
6. Проведения системных испытаний в реальных условиях;
7. Комплексного анализа результатов и вынесения заключения по результатам аттестации.

Аттестация производится в порядке, установленном "Положением по аттестации объектов информатизации по требованиям безопасности информации", утверждённым 25 ноября 1994 года. Относительно наиболее общих сфер деятельности предприятий государственным законодательством были разработаны

общие и обязательные для выполнения стандарты, на которых базируется аттестация информационного объекта.

При успешном прохождении всего комплекса испытаний выдаётся «Аттестат соответствия», на период времени, в течение которого будет обеспечена неизменность условий для осуществления деятельности, связанной с рабочим процессом, на объекте информатизации. Особое внимание уделяется технологическим решениям, связанным с обработкой информации и способным оказать чрезвычайное влияние на характеристики защищённости информационных ресурсов.

Одним из наиболее ярких примеров объекта информатизации, успешно прошедшего весь комплекс аттестационных испытаний, является ОАО «РЖД». В целях получения практических результатов была произведена проверка на соответствие средств и ресурсов, которые проходили комплекс аттестационных испытаний, с эксплуатируемыми в ходе рабочего процесса на момент исследования. По причине ограничения доступа к конфиденциальным ресурсам было возможно ознакомиться и исследовать следующие элементы объекта информатизации:

1. Антивирусная защита;
2. Обеспечение безопасности доменной политики;
3. Обеспечение безопасности каналов связи.

По итогам проверки было выявлено полное соответствие установленной политики безопасности компании действующему законодательству, что позволяет создать максимально защищённые условия работы с информационными ресурсами внутри информационной системы. Данное предприятие неоднократно доказывало полное соответствие нормативно-правовым актам обеспечения информационной безопасности, что позволяло эффективно использовать ресурсы разного рода (в частности, информационные) в своей деятельности и добиваться по итогу высоких результатов. Кроме того, периодическое прохождение аттестационных испытаний позволило предприятию активно развиваться и расширять спектр своей деятельности. Проанализировав этот пример, можно прийти к заключению, что требования, установленные на законодательном уровне и являющиеся теоретической базой обеспечения безопасности, полностью удовлетворяют практическим нуждам, при полноценной и корректной реализации которых возможно создать организованную и контролируемую систему безопасности, где будет

обеспечено надёжное хранение, передача и обработка информационных ресурсов разного уровня доступности.

Необходимо отметить, что одним из важных условий развития предприятия является его полная информатизация и внедрение цифровых и программных решений во все его сферы. Для осуществления данных действий на практике необходимо производить периодическую аттестацию объекта в целях повышения уровня защищённости информационных ресурсов предприятия. При проведении аттестации необходимо учесть все особенности данного комплекса мероприятий, представленные в соответствующих нормативно-правовых документах и установленные законодательством РФ. Выполнение описанных выше условий позволит обеспечить высокую эффективность рабочего процесса, модернизировать систему информационной безопасности и создать положительную тенденцию использования новейших научно-технических разработок, направленных на развитие сферы защиты информационных ресурсов.

Библиографический список

1. Положение по аттестации объектов информатизации по требованиям безопасности информации. (Утверждено Председателем Гостехкомиссии России 25.11.1994). – М.: Гостехкомиссия РФ, 1994, с. 22.
2. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. – М.: Горячая линия – Телеком, 2005, с. 416.
3. Сёмкин С.Н., Сёмкин А.Н. Основы правового обеспечения защиты информации. Учебное пособие для вузов. М - 238 с.: ил. 2008
4. Аттестация объекта информатизации по требованиям безопасности информации [Электронный ресурс]: Режим доступа: http://www.intuit.ru/studies/courses/2291/591/lecture/12685 – Загл. с экрана.
5. Железная дорога [Электронный ресурс]: Режим доступа: https://clck.ru/CFtAS – Загл. с экрана.