Дмитревская А.Д.
Научный руководитель: к.э.н., доцент Е.В. Родионова
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
E-mail: arina.murom@mail.ru

Обзор актуальных угроз информационной безопасности на предприятии

Массив информации, который обрабатывается в информационно телекоммуникационной системе ФНС России предоставляет потенциальную возможность для выявления угроз безопасности, которые в свою очередь, могут быть вызваны явлениями, процессами или действиями, провоцирующими причинение ущерба ФНС России [1].

Для объектов информатизации ФНС актуальными и основными источниками внешних антропогенных угроз безопасности информации являются [2]:

– технические разведки иностранного происхождения, направленные на сведения, содержащие государственную тайну и на ключевую систему информационной инфраструктуры выше третьего уровня;

– злоумышленники, которые осуществляют преднамеренное воздействие деструктивного характера на информационные ресурсы;

– криминальные и террористические элементы;

– подрядчики, производящие монтажные и наладочные работы технического оборудования информационных систем ФНС;

– поставщики программно-технических средств и услуг.

Основными источниками внутренних антропогенных угроз являются:

– сотрудники ФНС, действующие вне регламентированных полномочий, несущие преднамеренный характер угроз;

– сотрудники ФНС, действующие в рамках регламентированных полномочий, несущие непреднамеренный характер угроз.

К основным техногенным источникам угроз можно отнести неблагоприятные события техногенного характера, включая аварии на средствах телекоммуникационной инфраструктуры, на средствах инженерных коммуникаций, отказы и сбои в работе оборудования.

Для объектов ФНС актуальными уязвимостями являются [2]:

– ошибки, совершенные в процессе проектирования объектов информатизации налоговых органов и телекоммуникационной инфраструктуры, включая физический износ оборудования, относительно небольшой промежуток времени наработки на отказ техники и программного обеспечения;

– недостаточная техническая укрепленность и недостаточный уровень организации системы охраны налоговых органов, включая нарушения эксплуатации технических средств, таких как: жизнеобеспечения и энергообеспечения;

– особенности сотрудников морального и физического плана, которые могут являться предпосылками к криминальному или террористическому воздействию, к которым можно отнести: недовольство положением, недовольство действиями руководства, психологическая несовместимость некоторых сотрудников, психосоматическое и физическое состояние;

– восприимчивость программного обеспечения к вирусам и вредоносным программам;

– возможность несанкционированной модификации программных вызовов, кода, использование среды программирования автоматизированной информационной системы;

– уязвимости СиЗи (системы защиты информации);

– несоответствующая настройка конфигурации программного обеспечения с регламентирующей правовой базой, включая средства защиты информации, неконтролируемость их изменений, не декларированные действия сотрудников при управлении программным оборудованием;

На основе рассмотренных источников и уязвимостей ФНС России в широком смысле можно сформировать более конкретизированный перечень угроз. Количество таких угроз для ФНС России составляет более 200 единиц.

Методика определения уровня защищенности и актуальности той или иной угрозы также содержит определенные сложности. К одному показателю может подойти сразу несколько значений, а может не подойти ни одного, что также создает сложности в вычислениях. Актуальность угрозы также зависит от предпосылок, но неактуальные угрозы также должны быть включены в список угроз, но с нулевым значением вероятности, это предполагает произведение большого количества лишних расчетов для угроз, не имеющих никаких предпосылок.

Также вызывает сложности процесс определения показателя «опасность угрозы». Высокая, средняя и низкая опасность определяется в соотношении масштаба последствий, которые могут произойти при реализации той или иной угрозы. В соответствии с действующей методикой определить значимость или незначительность негативных последствий можно с помощью опроса экспертов. Анализ метода экспертной оценки, в свою очередь, показал большое количество недостатков использования данного метода. Данный метод отличается высоким уровнем субъективности оценки и наличием человеческого фактора, который может стать причиной определения степени опасности угрозы информационной безопасности, как низкой, с целью сокращения списка актуальных угроз [3].

Литература

1. Лиференко А.В. Модернизация автоматизированной информационной системы налогового учета в России // Актуальные проблемы авиации и космонавтики: межвузовский сборник научных трудов. 2016. №12. С. 67-69. – [Электронный ресурс] – https://elibrary.ru/item.asp?id=28146277 (дата обращения: 20.03.2022)

2. Кучеров И.И. Налоговая тайна в системе мер защиты конфиденциальной информации / Налоговое право России: учебник / отв.ред. Ю.А. Крохина. - 6-е изд., испр. - М.: Норма, 2015. С. 403 – [Электронный ресурс] – https://cyberleninka.ru/article/n/pravovoy-rezhim-zaschity-nalogovoy-informatsii-i-voprosy-ego-optimizatsii (дата обращения 25.03.2022);

3. Меховцева Е.В. Налоговая тайна: правовой режим охраны // Ленинградский юридический журнал. 2013. N 1. С. 38 - 42