УДК 004.056.53

ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОРГАНИЗАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА НАРУШИТЕЛЕЙ В ЗДАНИЯ И ПОМЕЩЕНИЯ

ASSESSMENT OF SECURITY OF INFORMATION RESOURCES OF THE ORGANIZATION FROM ILLEGAL ACCESS OF VIOLATORS TO BUILDINGS AND LOCATIONS

А.В. ТЕЛЬНЫЙ, Ю.М. МОНАХОВ, М.Ю. МОНАХОВ
A.V. TELNYY, YU.M. MONAKHOV, M.YU. MONAKHOV

(Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых)
(Vladimir State University named after Alexander and Nikolai Stoletovs)
E-mail: mmonakhov@vlsu.ru

В статье предлагается подход к оценке защищенности информационных ресурсов предприятия от несанкционированного доступа нарушителей в здания и помещения. В качестве основных показателей защищенности рассматриваются вероятность посягательства на охраняемый объект, вероятность срабатывания объектового комплекса технических средств охраны, вероятность реализации злоумышленником угрозы и вероятность задержания нарушителя физической охраной.

In article approach to an assessment of security of information resources of the enterprise from illegal access of violators to buildings and locations is offered. As the main indices of security the probability of infringement of the protected object, probability of actuating of an object complex of technical means of protection, probability of implementation by the malefactor of threat and probability of detention of the violator of physical protection are considered.

Ключевые слова: информационные ресурсы, защищенность информационных ресурсов, несанкционированный доступ нарушителей, инженерно-техническое укрепление, технические средства охраны, физическая охрана.

Keywords: informational resources, protection of information resources, unauthorized access to intruders, the strengthening of engineering, technical means of protection, physical security.

Вопросы исследования защищенности информационных ресурсов (ИР) в информационно-телекоммуникационных системах (ИТКС) предприятия, в том числе разработка методологических подходов к оценке показателей защищенности (конфиденциальности, целостности, достоверности и доступности) ИР в условиях информационных атак рассматриваются в [1...6]. В данных работах описываются процессы оценки защищенности ИР при электронном взаимодействии и в условиях информационного противодействия в корпоративной сети. Кроме непосредственно компьютерной безопасности для оценки защищенности ИР дополнительно необходимо оценивать защищенность самих зданий и помещений предприятия и организации, в которых циркулируют ИР и размещено оборудование их обработки, технические средства передачи информации (ТСПИ), хранятся носители ИР, работает персонал, использующий ИР. Уязвимыми к неправомерным действиям

нарушителей являются все перечисленные компоненты. В связи с этим оценке подлежит защищенность от несанкционированного доступа (НСД) нарушителей в данные здания и помещения.

Техническими средствами защиты от НСД нарушителей в здания и сооружения являются системы: инженерно-технического укрепления (ИТУ) элементов строительных конструкций; охранно-тревожной сигнализации (ОТС); контроля и управления доступом (СКУД); передачи тревожных извещений с объекта (СПИ) на пункт централизованной охраны (как часть охранной сигнализации). Кроме того, средством защиты от НСД нарушителей являются наряды физической защиты по выезду на охраняемый объект и задержанию нарушителя. Для оценки защищенности ИР от НСД нарушителей в охраняемые здания и сооружения будем использовать вероятностно-временные модели. Выделим частные показатели защищенности.

1. Вероятность посягательства на охраняемый объект (здание, сооружение) $P_{пос}$ – величина, характеризующая потенциальную криминальную опасность посягательства нарушителя на охраняемый объект. Может характеризоваться статистически средним количеством попыток проникновения за определенный период времени или оцениваться вероятностно, в виде функции:

$$P_{пос} = f_1(k_1, k_2, k_3), \qquad (1)$$

где k_1 – коэффициент, характеризующий состояния инженерно-технического укрепления элементов строительных конструкций. Чем более укрепленный объект, без видимых недостатков в укреплении, чем сложнее преодоление укрепления (взлом решеток, пролом стен, вскрытие замков и т.д.), тем меньше возможность нарушителя проникнуть на объект. Коэффициент, как правило, показывает уровень превентивной защиты от случайного, неопытного и несведущего нарушителя; k_2 – коэффициент, характеризующий ценность ИР посягательства – чем ценнее информационный ресурс для предприятия, тем выше вероятность желания нарушителей скопировать, модернизировать или уничтожить его; k_3 – коэффициент, характеризующий тип нарушителя.

Будем считать, что нарушители ранжируются по различному основанию:

- по степени подготовленности (случайный нарушитель, неподготовленный нарушитель, подготовленный нарушитель, специально подготовленный нарушитель);
- по степени информированности об объекте (нарушитель знает топологию объекта, нарушитель знает топологию и ТСО объекта, нарушитель имеет доступ к ИТУ объекта, нарушитель имеет доступ к ИТУ и ТСО объекта);
- по степени оснащенности специальными средствами проникновения (у нарушителя нет оснащения, у нарушителя имеется ручной инструмент, у нарушителя имеется электрический, пневматический (гидравлический) инструмент, у нарушителя имеется специальный инструмент);
− по виду прогнозируемого ущерба, который собирается нанести нарушитель.

Кроме того, вероятность посягательства на объект следует рассматривать в зависимости от способа посягательства, где такими способами могут быть:

- негласное проникновение одиночного постороннего нарушителя;
- негласное проникновение нарушителя-сотрудника предприятия;
- проникновение группы нарушителей в нерабочее время;
- проникновение одного или группы вооруженных нарушителей под видом посетителей;
- вооруженное нападение на объект.

Для оценки $P_{пос}$ может быть введено и более детальное градирование по коэффициентам (параметрам).

2. Вероятность $P_{ТСО}$ срабатывания объектового комплекса ТСО. Общая расчетная вероятность безотказной работы объектового комплекса ТСО производится раздельно по разным рубежам охраны:

$$P_{ТСО} = f_2(k_4, k_5, k_7, k_8), \qquad (2)$$

где k_4 – коэффициент, характеризующий вероятность безотказной работы всех

приемно-контрольных приборов со всеми задействованными шлейфами сигнализации и со всеми установленными на них извещателями. Более подробно методика определения данной величины изложена в [7]; k_5 – коэффициент, характеризующий вероятность безотказной работы канала связи между объектом и пунктом централизованной охраны (ПЦО); k_6 – коэффициент, характеризующий вероятность безотказной работы оператора АРМ и передачи информации о срабатывании ОТС наряду с физической охраной; k_7 – коэффициент, характеризующий вероятность последовательного саботажа всех охранных извещателей по маршруту передвижения до ИР; k_8 – коэффициент, характеризующий вероятность саботажа (подмены) приемно-контрольного прибора или канала связи с объекта до ПЦО.

3. Вероятность $P_{УГР}$ реализации злоумышленником угрозы. Каждый i-й вид угрозы требует от злоумышленника $t_{УГР\,i}$ времени нахождения в защищаемом помещении. Если нарушитель находился в помещении более $t_{УГР\,i}$, то можно считать, что угроза реализована. Вероятность реализации злоумышленником угроз ИР определяется величиной:

$$P_{УГР} = P(t \geq t_{УГР\,i}). \qquad (3)$$

Данную вероятность необходимо скорректировать с учетом вероятности задержания $P_{ЗАД}$ нарушителя физической охраной на объекте, которую можно рассматривать также как временной фактор: если время задержки от начала НСД до прибытия и действия наряда охраны – время задержания ($t_{ЗАД}$) – меньше времени, требуемого для проникновения на объект и реализации угрозы – время преодоления рубежей защиты ($t_{ПРЕОД}$):

$$P_{ЗАД} = P(t_{ЗАД} \leq t_{ПРЕОД}).$$

При этом реальное время задержания нарушителя $t_{ЗАД}$ складывается из: времени срабатывания ТСО; времени передачи сообщения тревоги на ПЦО; времени обработки тревоги АРМ; времени передачи сообщения о тревоге оператором (дежурным) наряду физической охраны; времени прибытия наряда на объект (самое большое время определяется дислокацией нарядов и объектов, дорожной обстановкой и т.д.); времени осмотра объекта и обнаружение проникновения; времени обнаружения нарушителя. Возможна и большая детализация по времени. Время преодоления рубежей защиты нарушителем $t_{ПРЕОД}$ складывается из: времени преодоления технического укрепления элементов строительных конструкций; времени преодоления (или саботажа) извещателей охранной сигнализации; времени нахождения нужного помещения и проникновение в него; времени реализации i-го вида угрозы $t_{УГР\,i}$.

Для объектов различных категорий должно существовать требуемое максимальное время задержки $t_{ТРЕБ}$, при котором с достаточной вероятностью нарушитель должен быть задержан. Таким образом, уровень защищенности ИР от НСД нарушителей в здания и помещения определяется выражением:

$$P_{ЗАЩ} = (1 - P_{ПОС})P_{ТСО}(1 - P_{УГР})P_{ЗАД}. \qquad (4)$$

Оценка значений параметров по пунктам 1...3 может быть проведена либо статистически по конкретному объекту или типу объекта, или дана в виде экспертных оценок. Критерий защищенности ИР в организации от НСД нарушителя в здания и помещения может определяется выражением:

$$P_{ЗАЩ} \geq P_{ТРЕБ},$$

где $P_{ТРЕБ}$ – требуемое значение защищенности ИР.

ВЫВОДЫ

На основании изложенного подхода можно проводить оценку защищенности информационных ресурсов от НСД для различного рода объектов. Выдвигая требования к изменению факторов,

влияющих на защищенность ИР, можно формировать мероприятия по повышению уровня их защищенности. Кроме того, появляется возможность оценки эффективности принимаемых мер и используемых средств защиты на объекте.

Л И Т Е Р А Т У Р А

1. *Монахов М.Ю., Кулаков М.А., Полянский Д.А.* Анализ и пути повышения защищенности корпоративной сети предприятия // Вестник Костромского гос. ун-та им. Н.А. Некрасова. – 2010, № 1. С. 70...72.

2. *Полянский Д.А., Монахов М.Ю.* Факторы, определяющие достоверность информации в АСУП текстильного предприятия // Изв. вузов. Технология текстильной промышленности. – 2014, № 4. С. 90...93.

3. *Монахов М.Ю., Полянский Д.А., Монахов Ю.М., Семенова И.И.* Концепция управления процессом обеспечения достоверности информации в ИТКС в условиях информационного противодействия // Фундаментальные исследования. – 2014, № 9-11. С. 2397...2402.

4. *Монахов М.Ю., Монахов Ю.М., Семенова И.И.* Модель управления процессом обеспечения достоверности информационных ресурсов в информационно-телекоммуникационных системах // Проектирование и технология электронных средств. – 2014, № 3. С. 34...40.

5. *Монахов Ю.М., Власова А.М.* Методика расчета нормированного критерия доступности телекоммуникационной сети // Динамика сложных систем - XXI век. – 2015, Т. 9. №3. С. 73...77.

6. *Мишин Д.В., Монахов М.Ю.* Приоритеты функциональных элементов в задачах администрирования корпоративных сетей передачи данных // Проектирование и технология электронных средств. – 2010, №4. С.15...19.

7. *Тельный А.В., Монахов М.Ю.* Формирование динамической модели оценки показателей надежности объектовых комплексов технических средств охранной сигнализации // Динамика сложных систем - XXI век. – 2015. Т. 9, № 4. С. 34...41.

R E F E R E N C E S

1. Monahov M.Ju., Kulakov M.A., Poljanskij D.A. Analiz i puti povyshenija zashhishhennosti korporativnoj seti predprijatija // Vestnik Kostromskogo gos. un-ta im. N.A. Nekrasova. – 2010, № 1. S. 70...72.

2. Poljanskij D.A., Monahov M.Ju. Faktory, opredeljajushhie dostovernost' informacii v ASUP tekstil'nogo predprijatija // Izv. vuzov. Tehnologija tekstil'noj promyshlennosti. – 2014, № 4. S. 90...93.

3. Monahov M.Ju., Poljanskij D.A., Monahov Ju.M., Semenova I.I. Koncepcija upravlenija processom obespechenija dostovernosti informacii v ITKS v uslovijah informacionnogo protivodejstvija // Fundamental'nye issledovanija. – 2014, № 9-11. S. 2397...2402.

4. Monahov M.Ju., Monahov Ju.M., Semenova I.I. Model' upravlenija processom obespechenija dostovernosti informacionnyh resursov v informacionno-telekommunikacionnyh sistemah // Proektirovanie i tehnologija jelektronnyh sredstv. – 2014, № 3. S. 34...40.

5. Monahov Ju.M., Vlasova A.M. Metodika rascheta normirovannogo kriterija dostupnosti telekommunikacionnoj seti // Dinamika slozhnyh sistem - XXI vek. – 2015, T. 9. №3. S. 73...77.

6. Mishin D.V., Monahov M.Ju. Prioritety funkcional'nyh jelementov v zadachah administrirovanija korporativnyh setej peredachi dannyh // Proektirovanie i tehnologija jelektronnyh sredstv. – 2010, №4. S.15...19.

7. Tel'nyj A.V., Monahov M.Ju. Formirovanie dinamicheskoj modeli ocenki pokazatelej nadezhnosti ob"ektovyh kompleksov tehnicheskih sredstv ohrannoj signalizacii // Dinamika slozhnyh sistem - XXI vek. – 2015. T. 9, № 4. S. 34...41.

Рекомендована кафедрой информатики и защиты информации. Поступила 05.05.16.