УДК 004.056.5

Н.И. Глухов, П.Н. Наседкин

Аналитика внутренних угроз информационной безопасности предприятий

Проводится анализ внутренних угроз информационной безопасности. В результате проведенного в данной работе анализа угроз, связанных с утратой информации, предлагается новый подход к оценке возможного ущерба на предприятиях через рассмотрение онтологической модели взаимосвязи основных концептов. На основании онтологической модели выведена обобщенная формула для оценки потенциального ущерба предприятиям, которая отражает зависимость оценки потенциального ущерба от угроз безопасности и их источников в разрезе каждого информационного актива и свойств информации. В настоящей работе перечислены основные источники угроз, виды информации, затраты на бюджет и основные проблемы контроля и противодействия внутренним угрозам информационной безопасности.

Ключевые слова: источники угроз, риски, онтологическая модель, аналитика внутренних угроз, утечки конфиденциальной информации.
doi: 10.21293/1818-0442-2021-24-1-33-41

В рамках данной работы проводимый анализ внутренних угроз информационной безопасности учитывает следующие классификационные признаки угроз, обусловленных:

1) размещением источника внутренних угроз;

2) потенциальным существенным ущербом в количественном выражении;

3) природой возникновения:

3.1) искусственных (субъективных) угроз среди которых выделим непреднамеренные (случайные) угрозы в разрезе ошибок персонала;

3.2) преднамеренных, т.е. умышленных угроз, обусловленных действиями людей.

3.3) типов угроз в соответствии с ГОСТом Р 50922–96 [1], таких как утечка информации, несанкционированное воздействие на информацию и ее носители, т.е. зависящих от целенаправленного или возможно непреднамеренного воздействия.

Основные проблемы информационной безопасности происходят по причине умышленных угроз, и как следствие являются главной причиной противоправных действий [9].

Отметим, что носителями внутренних угроз безопасности информации предприятий являются следующие источники угроз:

1. Персонал и работники подрядных организаций, допускающих ошибки при эксплуатации автоматизированных систем.

2. Бывшие, обиженные и действующие сотрудники предприятий, в действиях которых просматриваются либо элементы коррупционной составляющей, либо действия умышленного противоправного характера.

В настоящее время возросло количество умышленных угроз в области экономической деятельности предприятий на фоне снижения реальных доходов населения, сокращения персонала предприятий, и в целом обусловленной нестабильной ситуации на рынке труда, что отражается на настроениях и в поведении не только сотрудников многих компаний, но и лиц, не имеющих постоянных заработков, а также и криминальных структур. Опасаясь за собственное будущее, а возможно и в целях получения дополнительного дохода работники копируют доступную конфиденциальную информацию и нередко вступают в сговор с криминальными структурами и фирмами подрядных организаций или фирмами-конкурентами, при это еще работая на предприятиях. Все вышеперечисленные действия увеличивают в большей степени риски утечки конфиденциальной информации. Компании, озабоченные утечкой корпоративных секретов, начали активно инвестировать в безопасность, повышая собственную конкурентоспособность.

Объектом исследования настоящей статьи являются внутренние источники информационных угроз, возникающие в процессе экономической деятельности предприятий. Предметом исследования настоящей статьи в разрезе проводимой аналитики внутренних угроз информационной безопасности предприятий является разработка онтологической модели взаимосвязи основных концептов в аналитике внутренних угроз информационной безопасности предприятий на основе понятий модели безопасности по ГОСТ Р ИСО/МЭК 15408-1–2012 [2].

Онтологическая модель взаимосвязи основных концептов в аналитике внутренних угроз информационной безопасности предприятий и факторов влияния на оценку потенциального ущерба

В результате умышленных или непреднамеренных действий работников предприятия могут быть задействованы каналы утечки конфиденциальной информации, что в свою очередь создаст вероятность нанесения ущерба предприятию. **Потенциальный ущерб является важным звеном при расчетах, связанных с оценкой эффективности информационных угроз предприятию.** В рамках данной работы по анализу внутренних угроз мы будем исходить из построения онтологической модели взаимосвязи основных концептов в аналитике внутренних угроз информационной безопасности пред-

приятий и их влияния на оценки возможного ущерба предприятиям.

С позиции экономического подхода утечки конфиденциальной информации влияют на оценку возможного ущерба информационной безопасности предприятиям, в связи с чем возможный или потенциальный ущерб складывается из:

1. Прямого потенциального ущерба информационной безопасности предприятиям, который может возникнуть вследствие утечки конфиденциальной информации.

2. Косвенного возможного ущерба, т.е. текущих потерь, которые зависят от ограничительных мероприятий на распространение информации конфиденциального характера.

В основе описания прямого потенциального ущерба предприятиям в данной работе лежат количественные и качественные показатели, использующие экспертные оценки по обоснованию отнесения информации к конфиденциальной, а также оценки возможных сценариев развития событий и их последствий с учетом стоящих перед предприятиями целей и задач.

Ограничительные мероприятия на распространение информации конфиденциального характера, влияющие на расчет косвенного возможного ущерба, могут иметь положительные и отрицательные последствия, а именно:

1. Положительные, связанные с предотвращением потенциального прямого ущерба предприятию из-за утечки конфиденциальной информации.

2. Отрицательные, связанные с увеличением затрат на защиту информации и упущенную выгоду от ее открытого распространения, а также с увеличением вероятности косвенного потенциального ущерба.

Расчет потенциального ущерба предприятию с точки зрения информационной безопасности, связанного с утечкой конфиденциальной информации, на основании общего представления об оценке угроз производится в следующем порядке:

1. Вся информация на предприятии методом экспертного анализа и количественного оценивания ранжируется по степени важности, в том числе с учетом конфиденциальности.

2. В соответствии со степенью важности информации сравнивают входящие в нее сведения с количественной экспертной оценкой возможного ущерба, который может произойти с утратой данной информации.

Анализ научной литературы с учетом ГОСТ Р ИСО/МЭК 15408-1–2012 [2] позволил определить состав концептов в области понятий в аналитике внутренних угроз информационной безопасности предприятий, их взаимосвязей и влияния на возможный ущерб предприятий, что позволило построить онтологическую модель, представленную на рис. 1, которая может быть адаптирована и применена к различным предметным областям данного направления исследований. Онтологическая модель, представленная на рис. 1, выполнена в приложении «CmapTools» – это приложение, которое позволяет проектировать и легко создавать концепт-карты.

В соответствии с онтологией, представленной на рис. 1, просматривается влияние на расчет возможного ущерба (оценки суммарных издержек – S) следующих составляющих характеристик: количество рисков (угроз) для каждого информационного актива – N_{ij}, где номер угрозы $i=\overline{1,n}$; номер актива – $j=\overline{1,m}$; реализации угроз (оценки риска) в разрезе основных свойств информации (конфиденциальность, целостность, доступность) по каждому информационному активу – $A_{\text{к}}(i,j)$, $A_{\text{ц}}(i,j)$, $A_{\text{д}}(i,j)$, усредненное значение риска каждого информационного актива $A_{\text{ср}}(i,j)$.

С учетом вышесказанного влияние возможного ущерба на уровень общего риска всего предприятия основывается на следующих шагах:

Шаг первый. Оценка риска, определяемая через вероятность реализации угроз с учетом уязвимостей каждого элемента информационного актива в разрезе зависимости от вклада коэффициентов конфиденциальности, целостности, доступности, а также с учетом коэффициента разрушительности актива и частоты возникновения неблагоприятного события. Для первого шага можно привести следующие формулы [12, 13]:

$$A_{\text{к}}(i,j)=K_{\text{к}ij}\times P1_{ij}\times P2_{ij}\times V_{ij}\times R_{ij}, \qquad (1)$$

$$A_{\text{ц}}(i,j)=K_{\text{ц}ij}\times P1_{ij}\times P2_{ij}\times V_{ij}\times R_{ij}, \qquad (2)$$

$$A_{\text{д}}(i,j)=K_{\text{д}ij}\times P1_{ij}\times P2_{ij}\times V_{ij}\times R_{ij}, \qquad (3)$$

где (j) – определяемый информационный актив; $A_{\text{к}}(i,j)$ – значение риска конфиденциальности; $K_{\text{к}j}$ – коэффициент конфиденциальности информационного актива; $P1_{ij}$ – вероятность реализации угрозы; $P2_{ij}$ – вероятность использования уязвимости; $A_{\text{ц}}(i,j)$ – значение риска целостности; $K_{\text{ц}ij}$ – коэффициент целостности информационного актива; $A_{\text{д}}(i,j)$ – значение риска доступности; $K_{\text{д}ij}$ – коэффициент доступности информационного актива; V_{ij} – частота возникновения за фиксированный промежуток времени неблагоприятного события; $R_{ij}\in[0;1]$ – коэффициент разрушительности [12, 13].

Далее необходимо учесть среднее значение риска по информационным активам (1)–(3) в зависимости от угроз $i=\overline{1,n}$, где

$$A_{\text{ср}}(m,n)=\frac{1}{mn}\sum_{j=1}^{m}\sum_{i=1}^{n}(A_{\text{к}}(i,j)+A_{\text{ц}}(i,j)+A_{\text{д}}(i,j)), \qquad (4)$$

Предлагаемое отношение позволяет оценить значение риска и подсчитать стоимостные затраты при появлении инцидентов информационной безопасности.

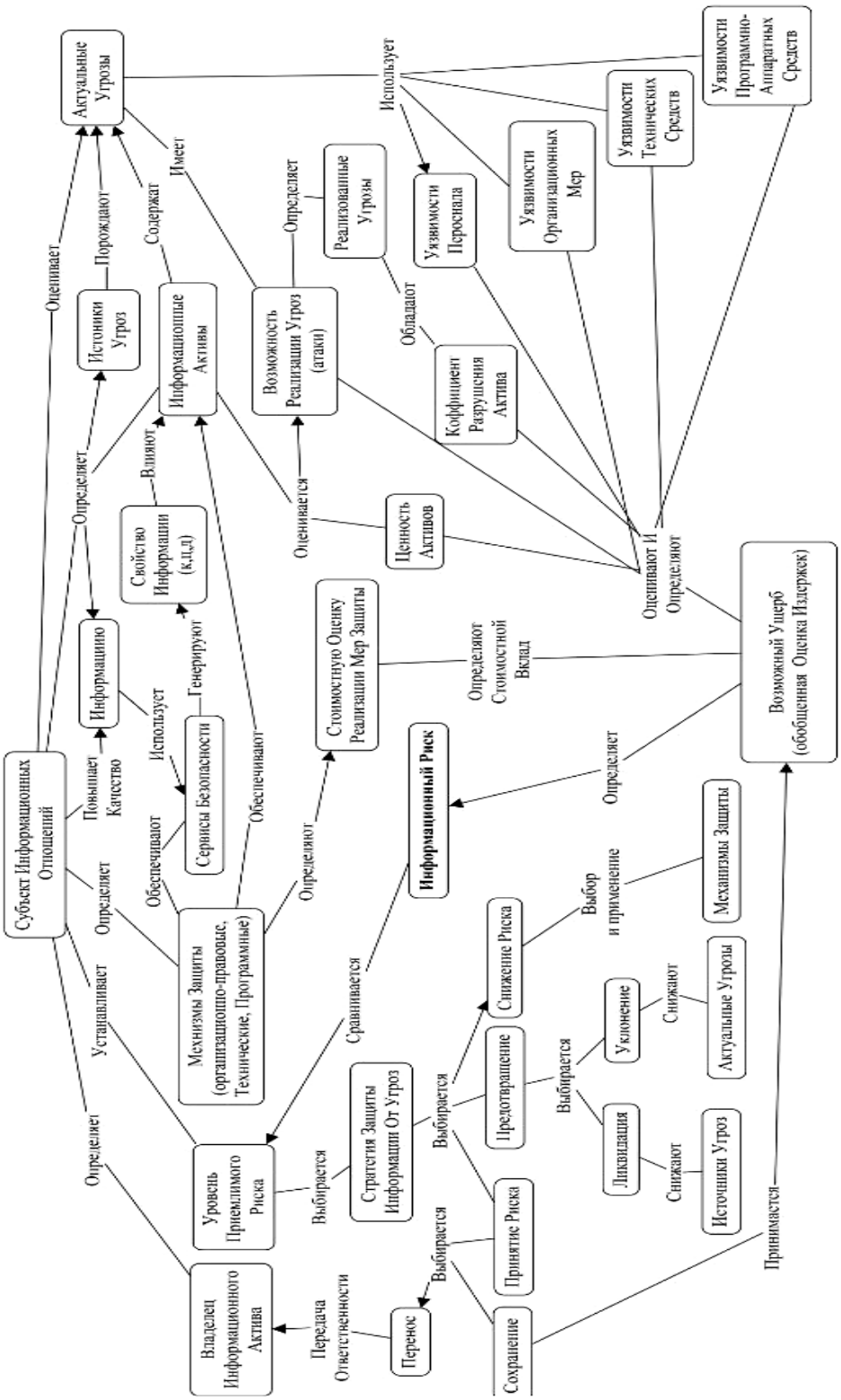

Рис. 1. Онтологическая модель предметной области

Шаг второй. На основании вышеописанного можем сделать предположение об обобщенной формуле оценки возможного ущерба (допустимых издержек) используя среднее значение риска, рассчитанного по каждому информационному активу и с учетом размера потенциальных потерь. Таким образом, значение ущерба $S(x)$ принимает следующий вид (5):

$$S(x) = S_0 + S_1 + S_2 + S_3 + S_4 + \sum_{j=1}^{m}\sum_{i=1}^{n}(A_{\text{ср}}(m,n)\times B_{ij} + C_{ij}), \quad (5)$$

где S_0 – параметр начальных затрат (издержек) на создание системы информационной безопасности предприятия; S_1 – параметр ежегодно планируемых затрат (издержек) на восстановление информационных активов; S_2 – параметр затрат (издержек) на

ежегодное сопровождение и техническое обслуживание информационных активов; S_3 – параметр планируемых ежегодных затрат (издержек) на внедрение новых информационных активов; S_4 – параметр ежегодных затрат (издержек) на службу безопасности предприятий; n – количество рисков (опасности определенной угрозы); m – количество информационных активов, «стоимостная оценка потерь (возможного ущерба) в случае реализации угрозы – B_{ij}; стоимостная оценка реализации мер защиты – C_{ij}.

Необходимо отметить, что существуют и другие подходы расчета ущерба информационной безопасности предприятий. Однако они в своей сути выполняют методику расчета с учетом определенных задач, не включающих все факторы влияния на оценку потенциального ущерба предприятия, к примеру, включают в одном случае оценку возможного ущерба автоматизированных систем (информационного ресурса) [11], а в другом случае оценку ущерба от реализации угроз, связанных с неправомерным доступом и использованием утечки персональных данных, в том числе включая штрафы за нарушение законодательства и стоимость на восстановление информационных ресурсов [14].

Далее рассмотрим текущее состояние в области обеспечения информационной безопасности в разрезе основных источников угроз, каналов утечки информации и их контроля, ущерба и затрат в рамках бюджета, выделяемых предприятиями на свою защиту информации.

Исследование основных направлений и показателей информационной безопасности 2019 г., влияющих на возможный ущерб от внутренних угроз компаний России и стран СНГ

В соответствии с аналитическим отчетом компании «СёрчИнформ» (Россия) за 2019 г. в области оценки уровня информационной защиты и подходов к вопросам информационной безопасности в России, странах СНГ были установлены источники внутренних угроз, которые приведены в табл. 1–3 [10]. В исследовании принимали участие 1 052 человека – это начальники, работники, эксперты отраслей, руководители организаций (коммерческой (76%), государственной (22%) и некоммерческой сфер (2%)). Исследованием охвачены такие отрасли экономики, как IT, нефтегазовый сектор, промышленность, логистическая сфера, кредитно-финансовая сфера, ритейл, здравоохранение и другие отрасли.

Все приводимые далее сравнительные статистические оценки (%) исследований необходимо понимать как некое распределение (выборку) с учетом охваченного количества работников и отраслей.

Как видно из приведенной аналитики, как в России, так и в странах СНГ подавляющее число источников угроз информационной безопасности приходится на рядовых работников предприятий (73/81% – соответственно Россия и СНГ) и уволенных (40/30% – соответственно Россия и СНГ).

Таблица 1

Источники угроз в России и странах СНГ

Распределение источников угроз по России и СНГ, %	Источники угроз								
	Менеджеры отдела снабжения	Бухгалтеры/ экономисты/ финансисты	IT-специалисты	Помощники руководителя/секретари	Логисты	Другое	Руководители	Рядовые	Уволенные
Компании России	34	24	19	13	10	45	27	73	40
Компании СНГ	32	33	23	20	9	51	19	81	30

Источники угроз кредитно-финансовой сферы, нефтегазового сектора, промышленности, строительства, логистической сферы, ритейла, здравоохранения и IT-компаний в разрезе персонала предприятий

Распределение источников угроз по отраслям, %	Источники угроз							
	Менеджеры отдела снабжения	Бухгалтеры/ экономисты/ финансисты	IT-специалисты	Помощники руководителя/секретари	Логисты	Другое	Руководители	Рядовые
Компании нефтегазовой сферы России	44	24	24	18	12	65	29	84
Промышленность России	46	24	14	12	10	38	30	70
Кредитно-финансовая сфера России	21	47	32	13	3	37	36	89
Ритейл России	69	13	16	0	25	50	48	93
Сфера ИТ России	32	27	39	13	12	36	13	91
Строительство России	26	31	19	10	10	31	29	79
Логистическая сфера России	42	14	19	14	36	11	19	89
Здравоохранение России	6	38	19	19	6	44	26	74

Таблица 3

Источники угроз кредитно-финансовой сферы, нефтегазового сектора, промышленности, строительства, логистической сферы, ритейла, здравоохранения и IT-компаний в разрезе рядовых работников предприятий

Источник угроз – персонал	Распределение источников угроз по отраслям, %							
	Компании нефтегазовой сферы России	Промышленность России	Кредитно-финансовая сфера России	Ритейл России	Сфера ИТ России	Строительство России	Логистическая сфера России	Здравоохранение России
Рядовые	84	70	89	93	91	79	89	74

При рассмотрении по восьми отраслям экономики в разрезе должностей работников предприятий выделяются с порогом не ниже 25% от распределения по источникам угроз, возникающим от работников следующие позиции:

1. Источники угроз ИБ, возникающие по вине менеджеров отделов снабжения. Основная доля угроз по ИБ от действий менеджеров отделов снабжения приходится на такие отрасли, как ритейл (69%); промышленность (46%), компании нефтегазовой сферы (44%), логистическая сфера (42%), сфера ИТ (32%), строительство (26%). Остальная часть источников угроз ИБ, возникающих от работников в разрезе отраслей, распределяется на других работников, исполняющих свой функционал согласно должностным инструкциям.

2. Источники угроз ИБ возникающие по вине работников бухгалтерии, экономистов, финансистов. Основная доля по данным источникам угроз ИБ приходится на такие отрасли, как: кредитно-финансовая сфера (47%), здравоохранение (38%), строительство (31%), сфера ИТ (27%).

3. Источники угроз ИБ, возникающие по вине ИТ-специалистов. Основная доля по данным источникам угроз ИБ приходится на сферу ИТ-услуг (39%); кредитно-финансовую сферу (32%).

4. Источники угроз ИБ, возникающие по вине работников служб логистики. Основная доля по данным источникам угроз ИБ приходится на логистическую сферу (36%) и ритейл (25%).

5. Источники угроз ИБ, возникающие по вине руководителей. Основная доля по данным источникам угроз ИБ приходится на такие отрасли, как: Ритейл (48%), кредитно-финансовая сфера (36%), промышленность (30%), нефтегазовая сфера (29%), строительство (29%), здравоохранение (26%).

6. Источники угроз ИБ, возникающие по вине рядовых сотрудников предприятий как источников угроз приходящихся на весь сектор экономики России, доля которых составляет не ниже 70%.

Согласно аналитическому отчету компании «СёрчИнформ» (Россия) за 2019 г. установлены утечки по видам информации, которые приведены в табл. 4 [10].

Таблица 4

Утечки по видам информации по отраслям кредитно-финансовой сферы, нефтегазового сектора, промышленности, строительства, логистической сферы, ритейла, здравоохранения и IT-компаний в разрезе работников предприятий

Распределение утечек по видам информации по отраслям экономики РФ и компаниям СНГ, в %	Утечки по видам информации				
	Информация о клиентах и сделках	Техническая информация	Персональные данные	Финансовая информация	Другое
Компании нефтегазовой сферы России	30	43	30	14	8
Промышленность России	47	44	24	29	8
Кредитно-финансовая сфера России	53	8	47	31	14
Ритейл России	59	10	10	44	3
Сфера ИТ России	38	27	22	15	5
Строительство России	37	35	12	30	9
Логистическая сфера России	51	9	14	23	9
Здравоохранение России	16	26	42	11	16
Компании России	35	25	23	19	8
Компании СНГ	31	14	28	20	20

Среди утечек на первом месте выделяются по странам СНГ и России следующие утечки: информация о клиентах и сделках (31 и 35% соответственно) и утечки персональных данных (28 и 23% соответственно), а также 25% утечек технической информации по России в раках проведенного выборочного исследования.

Среди утечек по отраслям экономики России наиболее значимое количество утечек приходится на:

1) персональные данные в сфере кредитно-финансовой сферы (47%) и здравоохранения (42%);

2) информацию о клиентах и сделках в сфере ритейла (59%), кредитно-финансовую сферу (53%), логистическую сферу (51%);

3) финансовую информацию в сфере ритейла (44%).

Как видно из аналитики суммарных утечек за 2019 г. по отраслям, представленных в табл. 5, выделяются утечки в сфере ритейла (92%) и утечки с порогом не ниже 60% от рассматриваемой выборки в разрезе таких отраслей, как: здравоохранение, кредитно-финансовая сфера, промышленность, логистическая сфера. Важно отметить, что утечки в компаниях нефтегазовой сферы находятся вблизи выбранного порогового значения утечек, как и в сфере строительства и ИТ, что дает нам сделать вывод о том, что работа в направлении обеспечения информационной безопасности на предприятиях данных

отраслей имеет приоритет и проводится, о чем свидетельствуют статистические данные, представленные в табл. 5.

Среди основных каналов утечек, выделенных в аналитическом отчете компании «СёрчИнформ» (Россия) за 2019 г., как следует из табл. 6, являются: электронная почта (42% – СНГ, 48% – Россия), устройства хранения и мобильные телефоны (46% – Россия, 48% – компании СНГ), мессенджеры и телефоны (29% – Россия, 33% – компании СНГ) [10].

Таблица 5

Суммарные утечки по компаниям России по отраслям кредитно-финансовой сферы, нефтегазового сектора, промышленности, логистической сферы, ритейлу, здравоохранению, строительству и IT-компаниям, а также общее количество утечек по компаниям СНГ

Суммарные утечки	Распределение суммарных утечек по отраслям экономики, %									
	Компании нефтегазовой сферы России, %	Промышленность России, %	Кредитно-финансовая сфера России, %	Ритейл России, %	Сфера ИТ России, %	Строительство России, %	Логистическая сфера России, %	Здравоохранение России, %	Компании России, %	Компании СНГ, %
Суммарные утечки по компаниям	60	67	68	92	54	54	63	69	59	50

Таблица 6

Каналы утечек компаний России, СНГ

Распределение каналов утечек по России и СНГ, %	Каналы утечек				
	Электронная почта	Устройства хранения и мобильные телефоны	Мессенджеры/ телефония	Документы, отправляемые на печать	Облачные хранилища
Компании России	48	46	29	20	18
Компании СНГ	42	48	33	20	14

В табл. 7 приведена аналитика инцидентов внутренней безопасности по отраслям, среди которых отмечаются следующие направления: попытки откатов (здравоохранение – 44%, ритейл – 42%, логистическая сфера – 41%, промышленность – 40%, строительство – 38%, сфера ИТ – 30%) и промышленного шпионажа / работы в пользу конкурентов (ритейл – 39%, строительство – 43%, промышленность – 37%).

Таблица 7

Другие инциденты внутренней безопасности

Распределение инцидентов по безопасности в компаниях России (отрасли) и СНГ, %	Инциденты внутренней безопасности				
	Попытки откатов	Промышленный шпионаж/ работа в пользу конкурентов	Саботаж	Создание фирмы-боковика	Другое
Компании России	30	24	17	11	14
Компании СНГ	25	25	18	3	26
Компании нефтегазовой сферы России	25	13	15	3	15
Промышленность России	40	37	15	16	10
Кредитно-финансовая сфера России	6	16	19	10	29
Ритейл России	42	39	31	19	3
Сфера ИТ России	30	26	11	8	18
Строительство России	38	43	16	16	14
Логистическая сфера России	41	28	16	22	3
Здравоохранение России	44	13	25	13	13

В настоящее время в бюджете на обеспечение информационной безопасности среди прочих систем защиты информации, используемых на предприятиях различных отраслей, согласно табл. 8, построенном по результатам аналитического отчета компании «СёрчИнформ» (Россия) за 2019 г., не используют в полном мере DLP-системы контроля и выявления утечек.

Однако особой строкой выделяются компании нефтегазовой отрасли (59%) и кредитно-финансовой сферы (53%), чьи службы безопасности активно внедряют и используют в своей работе DLP-системы контроля и выявления утечек, а следовательно, и эффективно противодействуют угрозам внутренней информационной безопасности предприятий [10].

Согласно табл. 9 построенного по результатам аналитического отчета компании «СёрчИнформ» (Россия) за 2019 г. в общем спектре ущерба по отраслям экономики и в сравнении общих показателей компаний России и СНГ существенным является имиджевый ущерб [10].

Согласно табл. 10 построенного по результатам аналитического отчета компании «СёрчИнформ» (Россия) за 2019 г. в общем спектре ущерба по отраслям экономики и в сравнении общих показателей компаний России и СНГ существенным являются мероприятия проводимые на предприятиях по контролю электронной почты, внешних носителей, программного обеспечения для администрирования, облачных хранилищ и документов отправляемых

на печать, телефонии и корпоративных мессенджеров [10].

Выводы и результаты исследований в области аналитики внутренних угроз информационной безопасности предприятий

На основании проведенной аналитики внутренних угроз информационной безопасности усовершенствован подход к оценке внутренних угроз с использованием разработанной онтологической модели взаимосвязей основных концептов. Ранее применение онтологической модели для исследования аналитики внутренних угроз предприятий с учетом детализации отношений между концептами информационной безопасности не использовался.

Таблица 8

Бюджет на обеспечение информационной безопасности среди прочих систем и средств защиты информации, используемых на предприятиях различных отраслей

Распределение бюджета по России и СНГ, %	Средства и системы ЗИ									
	Антивирусная программа	Средства администрирования Windows	NGFW (Firewall и Proxy)	Шифрование (криптошлюз, ПО)	DLP-система	Контроль целостности	IDS/IPS/EPS	SIEM-система	Другое	DCAP
Компании России	99	87	63	46	31	24	17	10	4	1
Компании СНГ	97	71	64	26	17	18	20	11	3	2
Компании нефтегазовой сферы России	100	92	80	57	59	31	33	25	8	4
Промышленность России	97	81	64	43	34	16	11	5	2	1
Кредитно-финансовая сфера России	100	91	80	76	53	56	40	22	2	4
Ритейл России	100	94	69	33	29	20	6	4	2	0
Сфера ИТ России	92	82	70	54	20	25	25	15	9	0
Строительство России	94	84	50	23	29	13	2	4	6	2
Логистическая сфера России	98	78	50	28	23	18	8	10	0	0
Здравоохранение России	96	93	64	71	21	36	18	0	0	4

Таблица 9

Виды ущерба по отраслям экономики России и СНГ

Распределение ущерба по России (по отраслям) и СНГ, %	Виды ущерба				
	Имиджевый ущерб	Compliance-риск (угроза наказания от регулятора)	Мелкий финансовый ущерб	Ущерба не было	Крупный финансовый ущерб
Компании России	40	13	39	30	13
Компании СНГ	39	17	43	35	19
Компании нефтегазовой сферы России	42	18	40	34	8
Промышленность России	43	9	50	23	16
Кредитно-финансовая сфера России	59	44	38	31	16
Ритейл России	26	8	67	26	21
Сфера ИТ России	54	13	50	32	8
Строительство России	35	11	35	35	19
Логистическая сфера России	35	6	38	38	21
Здравоохранение России	37	16	37	53	5

Таблица 10

Контроль ИТ-активов и документов по отраслям экономики России и СНГ

Распределение мер контроля по России (по отраслям) и СНГ, %	ИТ-активы и документы, подлежащие контролю									
	Корпоративная почта	Внешние носители	ПО для администрирования	Документы, отправляемые на печать	Телефония	Мессенджеры корпоративные	Общедоступная почта	Облачные хранилища	Мессенджеры общедоступные	Другое
Компании России	87	55	51	42	40	37	30	27	22	9
Компании СНГ	83	45	50	28	33	36	29	29	22	14
Компании нефтегазовой сферы России	90	72	51	63	27	37	31	27	24	6
Промышленность России	86	53	48	37	39	40	26	25	22	10
Кредитно-финансовая сфера России	93	82	44	58	40	51	47	29	29	4
Ритейл России	100	43	57	40	40	60	32	34	36	6
Сфера ИТ России	77	44	41	38	43	25	25	25	14	8
Строительство России	86	54	54	32	36	44	34	30	26	4
Логистическая сфера России	79	41	36	41	36	38	31	23	23	0
Здравоохранение России	84	52	60	52	52	24	32	20	20	12

На основании данной онтологической модели выведена обобщенная формула для оценки потенциального ущерба информационной безопасности для предприятий. Данная формула отражает зависимости оценки возможного ущерба от угроз безопасности и их источников в разрезе каждого информационного актива с учетом свойств информации.

Из результатов аналитических исследований за 2019 г., касающихся оценки уровня информационной безопасности в компаниях России и СНГ, следует, что:

1. Не все компании широко используют программно-технические системы контроля и мониторинга (DLP-системы) по противодействию внутренним угрозам, что в свою очередь ведет к значительным утечкам конфиденциальной информации и как следствие к значительному имиджевому ущербу предприятий.

2. Основным источником внутренних угроз информационной безопасности на предприятиях был и остается персонал, контроль которого должен осуществляться как со стороны непосредственного руководителя, так и со стороны кадровых служб и служб безопасности.

Литература

1. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения / Утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 3732013-ст. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/ 1200058320, свободный (дата обращения: 18.05.2020).

2. ГОСТ Р ИСО/МЭК 15408-1–2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – Ч. 1. Введение и общая модель / Утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 15 ноября 2012 г. № 814-ст. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/ 1200101777, свободный (дата обращения: 18.05.2020).

3. ГОСТ Р ИСО/МЭК 27002–2012. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности / Утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии 24 сентября 2012 г. № 423-ст. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200103619, свободный (дата обращения: 18.05.2020).

4. ГОСТ Р ИСО 31000–2010. Менеджмент риска. Принципы и руководство. – М.: Стандартинформ, 2012. – 24 с.

5. ГОСТ Р ИСО 31010–2011. Менеджмент риска. Методы оценки риска. – М.: Стандартинформ, 2012. – 74 с.

6. ГОСТ Р ИСО/МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М.: Стандартинформ, 2008. – 31 с.

7. ГОСТ Р ИСО/МЭК 27005:2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М.: Стандартинформ, 2011. – 94 с.

8. ГОСТ Р 53114–2008. Защита информации. Обеспечение информационной безопасности организации. Основные термины и определения. – М.: Стандартинформ, 2009. – 20 с.

9. Блинов А.М. Информационная безопасность: учеб. пособие. – СПб.: Изд. СПБГУЭФ, 2010. – 96 с.

10. Исследование уровня информационной безопасности в компаниях России и СНГ за 2019 год [Электронный ресурс]. – Режим доступа: https://searchinform.ru/research-2019, свободный (дата обращения: 17.04.2020).

11. Климов С.М. Методика оценки возможного ущерба от нарушения безопасности информации автоматизированной системы // Изв. ТРТУ. – 2003. – № 4 (33). – С. 27–31.

12. Легчекова Е.В. Метод расчета риска информационной безопасности / Е.В. Легчекова, О.В. Титов // Сб. науч. статей междунар. науч.-практ. конф. «Проблемы и перспективы электронного бизнеса». – Гомель: Изд-во Белорус. торгово-эконом. ун-та потребительской кооперации. – 2017. – С. 87–89.

13. Нестеров С.А. Анализ и управление рисками в сфере информационной безопасности [Электронный ресурс]. – Режим доступа: http://window.edu.ru/resource/443/57443, свободный (дата обращения: 18.05.2020). – СПб., 2007. – 1 эл. архив (nesterov-security.zip).

14. Управление рисками. Модель безопасности с полным перекрытием [Электронный ресурс]. – Режим доступа: https://www.intuit.ru/studies/courses/531/387/lecture/8990, свободный (дата обращения: 17.04.2020).

15. Шинаков К.Е. Минимизация рисков нарушения безопасности при построении системы защиты персональных данных: автореф. дис. … канд. техн. наук: 05.13.19. – Брянск, 2017. – С. 70–97.

16. ISO/IEC 27000-1:2018 Information technology – Service management. – Part 1: Service managment system requirements [Электронный ресурс]. – Режим доступа: https://www.iso.org/obp/ui/#iso:std:iso-iec:20000:-1:ed-3:v1:en, свободный (дата обращения: 18.05.2020).

17. ISO 31000:2018. Risk management – Guidelines [Электронный ресурс]. – Режим доступа: https://risk-academy.ru/download/iso31000/, свободный (дата обращения: 18.05.2020).

Глухов Николай Иванович
Канд. экон. наук, доцент каф. информационных систем и защиты информации (ИСиЗИ)
Иркутского государственного университета путей сообщения» (ИрГУПС)
Чернышевского ул., 15, г. Иркутск, Россия, 664074
Тел.: +7 (395-2) 63-83-99, доб. 01-30
Эл. почта: gni1953@mail.ru

Наседкин Павел Николаевич
Аспирант каф. ИСиЗИ ИрГУПС
Чернышевского ул., 15, г. Иркутск, Россия, 664074
Тел.: +7 (395-2) 63-83-99, доб. 77-74
Эл. почта: nasedkin_pn@irgups.ru

Glukhov N.I., Nasedkin P.N.

Analysis of internal threats to information security of enterprises

In this work the authors analyze the internal threats to information security. The article provides the research results ob-

tained by analyzing the threats related to the information losses and presents a new approach to estimate possible damage to an enterprise by considering an ontological model of interrelation of basic concepts. Based on the ontological model the generalized formula to estimate a potential damage to an enterprise has been developed. This formula reflects the dependence of estimation of a potential damage on safety threats and their sources from the point of view of each information asset and information properties. In the work the main sources of threats, kinds of the information, expenses for the budget and basic problems in control and counteraction to internal threats of information safety are listed.

Keywords: threat sources, risks, ontological model, internal threat analysis, confidential information leaks.
doi: 10.21293/1818-0442-2021-24-1-33-41

References

1. GOST R 50922-2006. Data protection. Basic terms and definitions. Available at: http://docs.cntd.ru/document/1200058320 (Accessed: May 05, 2020) (in Russ.).

2. GOST R ISO /IEC 15408-1–2012. Information technology. Security methods and tools. Criteria for assessing the security of information technology. Part 1. Introduction and general model. Available at: http://docs.cntd.ru/document/1200101777, (Accessed: May 05, 2020) (in Russ.).

3. GOST R ISO /IEC 27002–2012 Information Technology (IT). Security methods and tools. Code of norms and rules of information security management Available at: http://docs.cntd.ru/document/1200103619, (Accessed: May 05, 2020) (in Russ.).

4. GOST R ISO 31000–2010. Risk management. Principles and guidelines. Moscow, Standartinform, 2012, 24 p. (in Russ.).

5. GOST R ISO 31010–2011. Risk management. Risk assessment methods. Moscow, Standartinform, 2012. 74 p. (in Russ.).

6. GOST R ISO /IEC 27001–2006. Information technology. Security methods and tools. Information Security Management Systems. Requirements. Moscow, Standartinform, 2008. 31 p. (in Russ.).

7. GOST R ISO / IEC 27005:2010. Information technology. Security methods and tools. Information Security Risk Management. Moscow, Standartinform, 2011. 94 p. (in Russ.).

8. GOST R 53114–2008. Data protection. Ensuring the information security of the organization. Key terms and definitions. Moscow, Standartinform, 2009. 20 p. (in Russ.).

9. Blinov A.M. *Informacionnaya bezopasnost: ucheb. posobiye* [Information security]. SPb: SPbGUEF, 2010. 96 p. (in Russ.).

10. *Issledovanie urovnya informazionnoy bezopfsnosti v kompaniyach Rossia i SNG za 2019 god* [A study of the level of information security in companies in Russia and the CIS for 2019]. Available at: https://searchinform.ru/research-2019/ (Accessed: April 04, 2020) (in Russ.).

11. Klimov S.M. *Metodika ozenki vozmozhnogo ucherba ot narushenya bezopasnosty informazii avtomatizirovannoy sistemy* [Methodology for assessing the possible damage from information security breaches of the automated system]. Izvestia TRTU, 2003, no. 4 (33), p. 27–31 (in Russ.).

12. Legchekova E.V, Titov O.V *Metod rasheta riska informazionnoy bezopasnosty* [The method of calculating information security risk]. Collection of scientific articles of the international scientific-practical conference «Problems and prospects of electronic business». Gomel, Publishing House of the Belarusian Trade and Economic University of Consumer Cooperatives, 2017, p. 87–89 (in Russ.).

13. Nesterov S.A. *Analiz i upravlenie riskami v sfere informazionnoy bezopasnosty* [Analysis and risk management in the field of information security]. Available at: http://window.edu.ru/resource/443/57443, (Accessed: May 18, 2020). St. Petersburg, 2007, 1 email. Archive (nesterov-security.zip) (in Russ.).

14. *Upravlenye riskami. Model bezopasnosty s polnym perecrytiem*. [Risk management. Security model with full overlap]. Available at: https://www.intuit.ru/studies/courses/531/387/lecture/8990 (Accessed: May 18, 2020) (in Russ.).

15. hinakov K.E. *Minimizazia riskov narushenya bezopasnosty pri postroenyii sistemyzachity personalnych dannych: avtoreferat dissertazii* [Minimizing the risks of security breaches when building a personal data protection system]. Bryansk, 2017. P. 70–97 (in Russ.).

16. ISO / IEC 27000-1: 2018. Information technology – Service management. Part 1: Service management system requirements. Available at: https://www.iso.org/obp/ui/#iso: std: iso-iec: 20000: -1: ed-3: v1: en. (Accessed: May 18, 2020).

17. ISO 31000:2018. Risk management. Guidelines. Available at: https://risk-academy.ru/download/iso31000/ (Accessed: May 18, 2020).

Nikolay I. Glukhov
Candidate of Science in Economics, Associate Professor,
Chair of Information Systems and Information Protection.
Irkutsk State Transport University (ISTU)
15, Chernyshevsky st., Irkutsk, Russia, 664074
Phone: +7 (395-2) 63-83-99, ext. 01-30
Email: gni1953@mail.ru

Pavel N. Nasedkin
Postgraduate student, Department of Information Systems and Information Protection, ISTU
15, Chernyshevsky st., Irkutsk, Russia, 664074
Phone: +7 (395-2) 63-83-99, ext. 77-74
Email: nasedkin_pn@irgups.ru