УДК 004.588 Вестник УрФО № 2(44) / 2022, с. 70–79

Астахова Л.В., Волегов Н.В.

DOI: 10.14529/secur220210

ДИНАМИКА ПОРТРЕТА ВНУТРЕННЕГО НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Инциденты информационной безопасности по вине внутреннего нарушителя обладают мощным разрушительным потенциалом. Последствия случайных ошибок или злонамеренных действий персонала могут проявляться не только в имущественных или репутационных потерях, но и в приостановке или ликвидации бизнеса как такового. Внутренний нарушитель не остается неизменным, вектор его действий меняется в связи с социокультурными трансформациями, развитием технологий организации информационных систем компаний, изменением локальных проблем объекта. Цель статьи – выявить изменения характеристик внутреннего нарушителя информационной безопасности организации за последние годы, их обусловленность. С помощью сравнительного анализа экспертных оценок за 2016-2021 годы в статье выявлены некоторые тенденции, которые наиболее ярко отражают динамику характеристик внутреннего нарушителя безопасности информационной системы: снижение утечек по вине внутреннего нарушителя в связи с распространением заболевания COVID-19; рост числа умышленных внутренних утечек защищаемой информации; стабильное доминирование случайных утечек персональных данных, по сравнению с умышленными, их медленное снижение; рост числа утечек по вине подрядчиков. Показаны возможные причины возникновения названных тенденций и некоторые пути решения проблем. Обоснована необходимость расширения критериев оценки внутренних нарушителей за счет мотивационных факторов, что позволит существенно повысить прагматическую ценность статистических экспертно-аналитических отчетов для практики защиты информации в организациях.

Ключевые слова: *внутренний нарушитель, информационная безопасность, организация, человеческие риски, критерии оценки, осведомленность, вовлеченность.*

DYNAMICS OF INTERNAL INTERVENTOR PORTRAIT INFORMATION SECURITY OF THE ORGANIZATION

Information security incidents due to the fault of an insider have a powerful destructive potential. The consequences of accidental errors or malicious actions of personnel can manifest themselves not only in property or reputational losses, but also in the suspension or liquidation of the business as such. An insider does not remain unchanged, the vector of his actions changes in connection with socio-cultural transformations, the development of technologies for organizing information systems of companies, and changes in the local problems of the object. The purpose of the article is to identify changes in the characteristics of an internal violator of the information security of an organization in recent years, their conditionality. Using a comparative analysis of expert assessments for 2016-2021, the article reveals some trends that most clearly reflect the dynamics of the characteristics of an internal violator of information system security: a decrease in leaks due to the fault of an internal violator due to the spread of COVID-19 disease; an increase in the number of intentional internal leaks of protected information; stable dominance of accidental leaks of personal data, compared with intentional ones, their slow decline; an increase in the number of accidental leaks of state secrets; an increase in the number of leaks caused by contractors. Possible causes of these trends and some ways to solve problems are shown. The necessity of expanding the criteria for assessing insiders due to motivational factors is substantiated, which will significantly increase the pragmatic value of statistical expert-analytical reports for the practice of information security in organizations.

Keywords: *insider, information security, organization, human risks, evaluation criteria, awareness, involvement.*

Введение. На протяжении длительного периода наблюдений в корпоративных информационных системах обнаруживается множество опасных уязвимостей, связанных с внутренними нарушителями информационной безопасности (ИБ). Их реализация приводит к существенным финансовым и репутационным потерям организации. Большое влияние на портрет внутреннего нарушителя не могут не оказывать социально-культурные трансформации общества, изменения в отрасли ИБ. Этим обусловлена цель статьи – выявить изменения характеристик внутреннего нарушителя информационной безопасности организации в условиях социально-культурной эволюции последнего времени, обосновать их причины и показать императивы управления организационным поведением сотрудников для предотвращения инцидентов ИБ по их вине.

Современные тенденции изменений характеристик внутреннего нарушителя. Нарушитель информационной безопасности организации (нарушитель)– физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации [1, п. 3.3.5]. Внутренние нарушители – нарушители, имеющие права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей [2, п.5.1.6]. При оценке возможностей внутренних нарушителей необходимо учитывать принимаемые оператором орга-

низационные меры по допуску субъектов к работе в информационной системе. Возможности внутреннего нарушителя существенным образом зависят от установленного порядка допуска физических лиц к информационной системе и ее компонентам, а также мер по контролю за доступом и работой этих лиц. Внутренний нарушитель может действовать как умышленно (преднамеренно), так и нет (неумышленно, непреднамеренно).

Результаты анализа ежегодных исследований российских и зарубежных аналитических центров свидетельствуют о том, что количество инцидентов ИБ по вине внутренних нарушителей не является неизменным. Так, мониторинг ежегодных отчетов Экспертно-аналитического центра компании InfoWatch за 2016-2021 годы позволил нам выявить динамику внутренних утечек, которую мы представили в графическом виде на Рис.1.

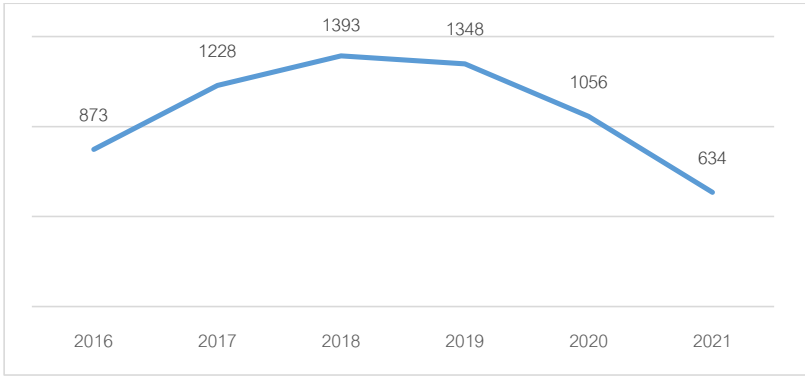

Рис. 1. Динамика утечек информации по вине внутреннего нарушителя информационной безопасности за 2016-2021 гг

Как видим, рост числа внутренних утечек, зафиксированный в 2016-2018 годах, в 2019 году сменился снижением. В 2020-2021 годах мы наблюдаем дальнейшее снижение числа утечек, т.к. в 2021 году утечки снизились на 53% по сравнению с 2019. В результате умышленных и случайных действий внутренних нарушителей произошло 36,8% утечек в 2021 г. и 47,1% в 2020 г. Если в 2018 г. на долю внутренних нарушителей пришлось примерно 2/3 случаев, то по итогам 2021 г. картина получилась практически зеркальной – почти в 2/3 всех внесенных опубликованных (ставших известными) утечек информации ограниченного доступа в качестве виновников указаны внешние нарушители. По мнению экспертов, большую роль сыграло распространение удаленной работы в период пандемии, когда контроль за сотрудниками оказался сильно затруднен. Недобросовестные работники могли незаметно похищать информацию, большой пласт случайных нарушений также мог остаться незамеченным [3]. Неуклонный рост доли числа внешних утечек, по сравнению с внутренними, эксперты связывают также: со становлением широкого спектра хакерских группировок; повышением доступности вредоносного ПО; вступлением сотрудников в сговор с хакерами; ошибками сотрудников, которые привели к раскрытию аутентификационной информации, которой воспользовались внешние нарушители; сокрытием информации о внутренних нарушителях и пробелах в организации безопасной удалённой работы и защитой своего имиджа и невозможностью перепроверить результаты их отчётов.

Интересен вопрос отношения количества умышленных утечек к случайным. В 2020 и 2021 году доля умышленных нарушений среди утечек внутреннего характера (по вине персонала) составляет более 51%. При этом доля умышленных нарушений внутреннего характера в мире растет: если в 2018 году это было 35,3%, то в 2021 – уже 51,8%. Ликвидность конфиденциальной информации становится все выше, что позволяет внутренним злоумышленникам ее монетизировать.

Главным объектом внимания внутренних нарушителей в течение 2016-2021 гг. стабильно являются персональные данные, о чем свидетельствует построенная диаграмма (Рис.2).

Очевидно, что ежегодно с 2016 года утечки персональных данных весьма сильно доминируют над утечками других видов данных. Интерес к платежной информации становится меньше, но тенденция роста наблюдается к коммерческой тайне.

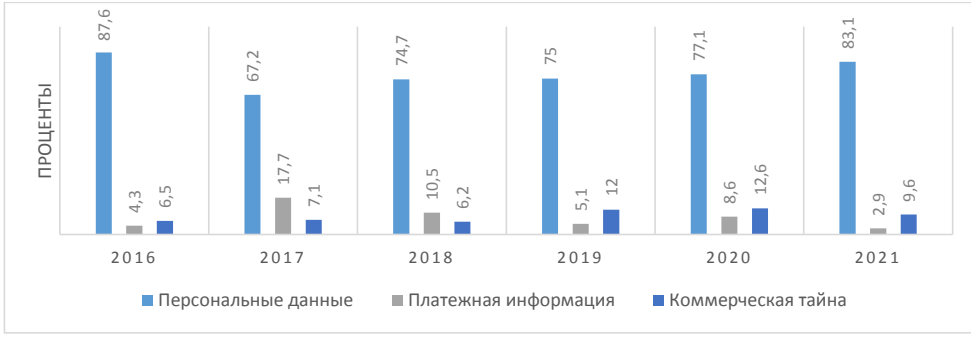

Рис.2. Распределение внутренних утечек по типу данных за 2016-2021 гг

Проведя сравнительный анализ экспертных исследований за разные годы [3], [4] и [5], мы пришли к выводу, что причины утечек разных видов данных существенно разнятся. Так, если в 2017-208 годах наблюдалось больше случайных утечек платежной информации, то с 2019 года доминируют умышленные утечки(Рис.3).

Полагаем, что внимание к повышению осведомленности сотрудников финансовых подразделений организаций принесло определенные плоды.

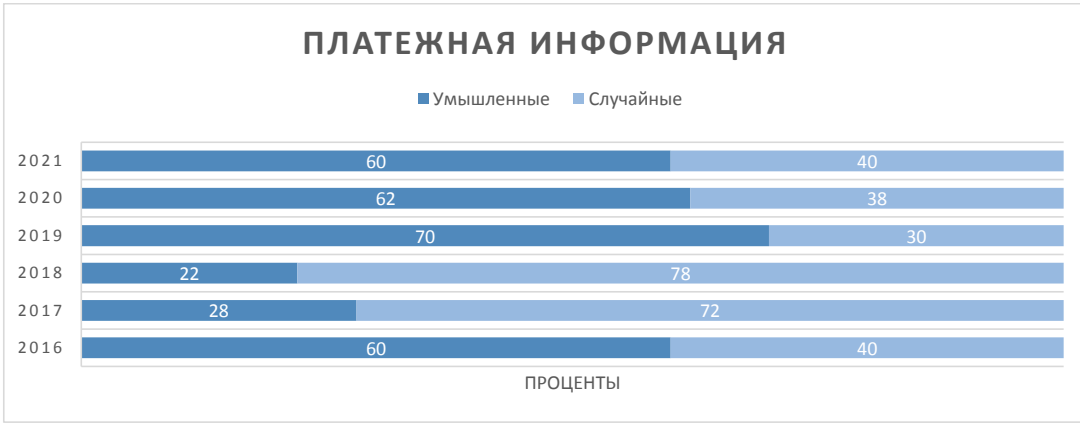

Рис.3. Распределение утечек платежной информации по умышленным и случайным

Этого нельзя сказать о персональных данных, их случайные утечки стабильно доминируют с 2016 года (Рис.4).

Это говорит о том, что далеко не все сотрудники организации, допущенные к обработке персональных данных в организации, столь же осведомлены о правилах ИБ и ответственны в процессе выполнения своих долж-

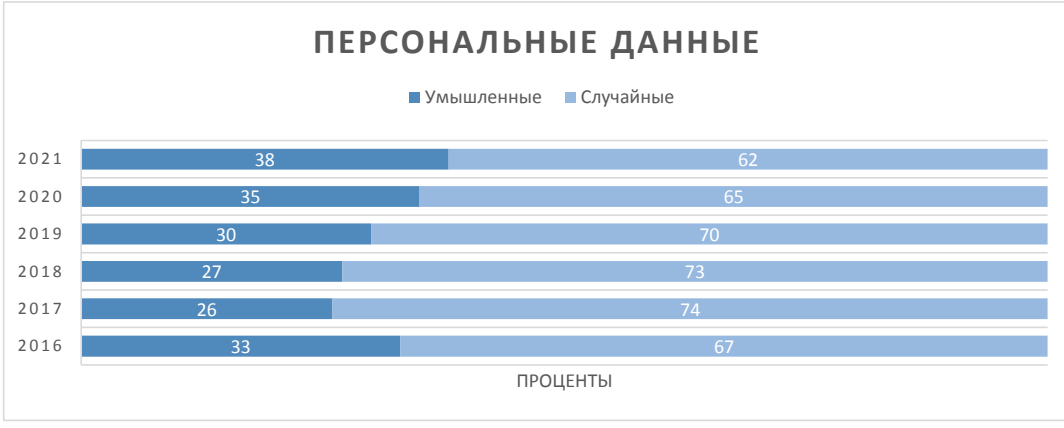

Рис.4. Распределение утечек персональных данных по умышленным и случайным

ностных обязанностей. Процесс повышения осведомленности идет медленно, хотя при этом и наблюдается небольшое плавное снижение случайных утечек.

Анализ отчетов InfoWatch [3], [4] и [5] позволил нам конкретизировать типы внутреннего нарушителя. Результаты анализа приведены на Рис.5.

Рис.5. Распределение внутренних утечек по виновнику

Из диаграммы видно, что лидером по нарушениям является рядовой сотрудник, поэтому из года в год актуальным остается проблема осведомленности и инструктаж персонала. К сожалению, по-прежнему во многих компаниях у руководства не находится времени или желания повышать осведомленность сотрудника или делать выбор сотрудников более тщательным на этапе их приема на работу. На втором месте по инцидентам ИБ из числа внутренних нарушителей находятся лица из числа персонала подрядных организаций, осуществляющих обработку информации ограниченного доступа по заданию коммерческой компании или государственной организации и допустивших утечку такой информации (в период действия контракта). Мало кто говорит про действия подрядных организаций, в основном внимание уходит на рядовых сотрудников и хакеров. Уделять внимание выбору подрядчика и его осведомленности об ИБ в процессе деятельности на объекте также важно, как и работа с рядовым сотрудником. С 2017 года усиливается тенденция роста утечек по вине руководителя, а также уменьшения числа утечек по вине системного администратора.

К сожалению, экспертные отчеты участников мирового аналитического рынка не содержат оценки характеристик внутренних нарушителей по социально-демографическим и психологическим критериям, без которых невозможно понять динамику их портрета под воздействием тех или иных мотивационных факторов.

Поэтому статистическая информация может быть дополняться результатами исследований, проводимых с помощью DLP-систем. Так, исследование «Ростелеком-Солар», направленное на создание типичного портрета сотрудника-нарушителя, проводилось с помощью DLP-системы SolarDozor и модуля анализа поведения с 2018 по 2020 год в 150 российских организациях в 20 отраслях и направлениях деятельности с различной численностью сотрудников[6, 7].

Результаты исследования по ряду аспектов характеристики внутренних нарушителей представим в виде круговых диаграмм (Рис. 6 и 7). 55% всех нарушителей – это мужчины, 58% – до 40 лет (Рис.6), 46% имеют стаж выше 5 лет (Рис.6).

При этом нарушители мужского пола молодого возраста подрабатывают в основное рабочее время, женского – рассылают резюме, публикуют их на сервисах по поиску работы. 26% нарушений приходится на сотрудников в возрасте 40–50 лет. Мужчины этого возраста используют много рабочего времени для посещения развлекательных ресурсов, а женщины - так же занимаются поиском новой работы. Кроме того, нарушители-женщины пересылают данные (в том числе личные и данные об оплате труда в организации) на внешние почтовые адреса. Эту особенность эксперты объясняют тем, что в бухгалтериях и отделах кадров (т.е. в подразделениях, где хранится эта информация), в России традиционно работают в основном женщины.

К сожалению, эксперты не предпринима-

Рис 6. Распределение увольнений в связи с инцидентами по возрасту

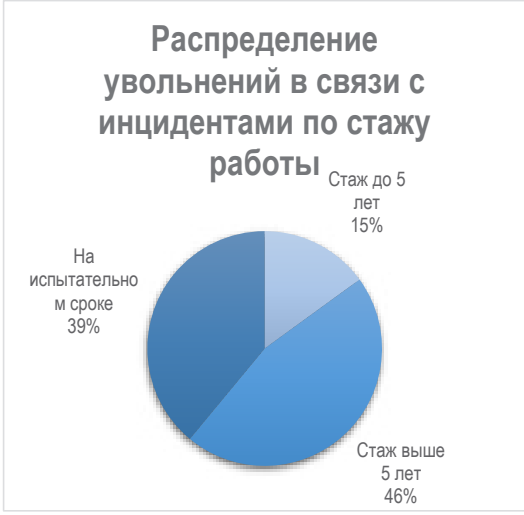

Рис. 7. Распределение увольнений в связи с инцидентами по стажу работы

ют более детального статистического анализа - мотивации внутреннего нарушителя ИБ организации, что существенно тормозит процессы мониторинга динамики его характеристик. Между тем, мотивы неправомерного поведения играют жизненно важную роль в области внутренних угроз информационной безопасности, и выявление мотивационных факторов и их классификация могут помочь руководству контролировать и уменьшить внутренние угрозы в организациях. На это обращают внимание зарубежные и российские эксперты.

Согласно классической структуре угроз защищаемой информации причинами, вызывающими преднамеренное дестабилизирующее воздействие, могут быть: стремление получить материальную выгоду (подработать), нанести вред (отомстить) руководству или коллеге по работе, а иногда и государству, оказать бескорыстную услугу приятелю из конкурирующей фирмы, продвинуться по службе, обезопасить себя, родных и близких от угроз, шантажа, насилия или показать свою значимость. А предпосылками, способствующими появлению этих причин, как правило, бывают: тяжелое материальное положение, финансовые затруднения; корыстолюбие, алчность; склонность к развлечениям, пьянству, наркотикам; зависть, обида; политическое или научное инакомыслие; личные связи с представителями конкурента; недовольство служебным положением, карьеризм; трусость, страх; тщеславие, хвастовство и др. [8]. Иные предпосылки – отсутствие интереса к работе, недооценка своих возможностей и способностей, плохое отношение со стороны администрации и др. - у причин непреднамеренных воздействий сотрудников на защищаемую информацию, к которым относятся безответственность, недисциплинированность, болезнь, переутомление и т.д. Исследования зарубежных экспертов [9] и [10] также связаны с анализом общих признаков и предпосылок неправомерных воздействий внутренних нарушителей на защищаемую информацию.

На основе приведенных результатов анализа статистической информации и экспертных мнений мы можем очертить штрихи к примерному портрету современного внутреннего нарушителя ИБ. Им является мужчина до 40 лет, со стажем более 5 лет или же он находится на испытательном сроке. Его социальные связи внутри коллектива слабы, а плохая привязанность к компании подталкивает его к поиску новой работы или нецелесообразному использованию времени на рабочем месте, у него нет достижений, плохая репутация, а его личностные нормы не соответствуют общепринятым в компании. Его должность относится к той, которая не подразумевает ответственности за обеспечение безопасности объекта, а значит – потенциальный нарушитель не заинтересован в противодействии утечкам, его заработная плата не зависит от количества утечек в организации. Это увеличивает вероятность как умышленных, так и неумышленных воздействий на защищаемую информацию. Названные ха-

рактеристики внутреннего нарушителя подтверждаются приведенными выше статистическими данными: слабая привязанность сотрудника к компании-работодателю и нахождение сотрудника на должности, которая не предполагает заинтересованности в информационной безопасности объекта. К числу таких сотрудников-нарушителей относятся: новый работник в компании, работник, собирающийся увольняться, или работник из подрядной организации. Все эти типы входят в тройку тех сотрудников, из-за которых чаще всего возникают утечки. Должности такого типа сотрудников не предполагают вовлеченности в обеспечение безопасности информационных систем.

Как видим, гуманитарная оценка портрета внутреннего нарушителя и выводы, полученные в процессе авторского статистического анализа утечек по его вине, совпадают. Данный вывод позволяет заключить, что руководство организации не может не обращать внимание на факторы внутренней и внешней среды, которые побуждают сотрудников к неправомерному поведению в области информационной безопасности. Поэтому все большее значение для снижения числа инцидентов ИБ организации по вине внутреннего нарушителя приобретает расширение критериев оценки анализа субъектов инцидентов ИБ за счет их гуманитарных характеристик. Тем более, что стремительное развитие российских и зарубежных DLP-систем дает возможность расширить количество этих критериев, формализовать их и включить в качестве объектов исследования экспертно-аналитических подразделений. Так, задачей, которую можно решить с помощью DLP-системы, является выявление групп риска — т. е. работников, имеющих склонности, увлечения, которые использованы для ведения или привлечения к незаконной деятельности, к деятельности в ущерб компании, её руководству или работникам [11]. Выявление признаков конфликта интересов также входит в перечень задач DLP-систем. По сути степень совпадения ценностей сотрудников с ценностями компании – это вовлеченность персонала. В это понятие входит позитивное психологическое состояние работника: энергичность, готовность приложить усилия при возникновении трудностей, преданность делу, вдохновение, гордость, полная концентрация на обязанностях [12]. Поскольку термин «вовлеченность» обладает «большей описательной силой и очевидной валидностью», именно его используют вместо таких терминов, как «удовлетворенность работой», «приверженность» и «мотивация» [13]. Вовлеченность сотрудника в работу организации является трендом современной практики работы с персоналом во всех отраслях деятельности и важнейшим фактором повышения осведомленности сотрудников об ИБ организации [14]. Кроме того, уже накоплен определенный опыт работы с данными ИБ-систем для оценки вовлеченности сотрудников [15]. Все это обусловливает необходимость в изменении подходов к статистическим аналитическим исследованиям в области информационной безопасности. Полагаем, что использование интегративной концепции внутренней угрозы (как возможности нарушения правил ИБ и мотивации внутреннего нарушителя в организации) позволит углубить содержание экспертно-аналитических отчетов по инцидентам ИБ в организациях различных типов и видов и усилить их эвристический и прогностический потенциал для практики защиты информации.

Вывод. Внутренние утечки обладают мощным разрушительным потенциалом. Последствия ошибок или злонамеренных действий персонала могут проявляться не только в имущественных или репутационных потерях, но и в приостановке или ликвидации бизнеса как такового. В определенные периоды наблюдаются изменения тенденций утечек по вине внутреннего нарушителя. Вектор его действий меняется в связи с внедрением новых технологий организации информационных систем компаний, динамикой локальных проблем объекта и др.

Анализ экспертных оценок за 2016-2021 годы позволил нам выявить несколько тенденций, которые наиболее ярко отражают динамику характеристик внутреннего нарушителя безопасности информационной системы. Снижение утечек по вине внутреннего нарушителя вызвано распространением заболевания COVID-19, переводом персонала в дистанционный режим работы, ограничением доступности физических каналов утечки (кража или утеря документов, взлом сейфов) и является временным явлением. Рост числа умышленных внутренних утечек защищаемой информации, вызванных взаимной неудовлетворенностью друг другом работодателя и работника, требует усиления самореализации и вовлеченности последнего в процесс

реализации бизнес-целей организации. Стабильное доминирование случайных утечек персональных данных, по сравнению с умышленными, их медленное снижение свидетельствует о необходимости повышения эффективности повышения осведомленности сотрудников об ИБ организации и культуры ее ИБ. Рост числа утечек по вине подрядчиков должен стимулировать работодателя тратить больше сил на повышение осведомленности этих категорий работников и правовые аспекты взаимодействия с ними.

Сам процесс выявления динамических характеристик внутреннего нарушителя – это процесс, требующий сегодня инновационных подходов. Развитие теоретических аспектов исследований внутреннего нарушителя, углубление факторного анализа его поведения, а также развитие инструментальных информационных технологий его мониторинга в организации – все это свидетельствует о необходимости изменения методологии создания статистических аналитических исследований в области информационной безопасности. Расширение критериев оценки внутренних нарушителей за счет мотивационных факторов позволит существенно повысить прагматическую ценность использования аналитических отчетов в практике защиты информации.

Литература

1. ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения (утв. и введен в действие Приказом Ростехрегулирования от 18.12.2008 N 532-ст). – URL: https://docs.cntd.ru/document/1200075565 (дата обращения: 11.04.2022).

2. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 года. – URL: https://docs.cntd.ru/document/607699443?section=text (дата обращения: 11.04.2022).

3. Отчёт об исследовании утечек информации ограниченного доступа в 2021 году / Экспертно-аналитический центр InfoWatch. – 2022. – 32. с. – URL: https://www.infowatch.ru/analytics/analitika/v-2021-stalo-bolshe-umyshlennykh-utechek (дата обращения: 12.04.2022).

4. Исследование утечек информации ограниченного доступа в 2020 году / Экспертно-аналитический центр InfoWatch. – 2021. – 30. с. – URL: https://www.infowatch.ru/analytics/analitika/issledovanie-utechek-informatsii-ogranichennogo-dostupa-v-2020-godu (дата обращения: 12.04.2022).

5. Утечки данных организаций по вине или неосторожности внутреннего нарушителя. Сравнительное исследование. 2013-2019 гг. / Экспертно-аналитический центр InfoWatch. – 2020 – 32. с. – URL: https://www.infowatch.ru/analytics/analitika/utechki-dannykh-po-vine-vnutrennego-narushitelya-2013-2019-gg (дата обращения: 12.04.2022).

6. Ростелеком-Солар. Кто он – типовой нарушитель в российской организации? 2018-2020 / Ростелеком-Солар. – 2021. – 12 с. – URL:https://rt-solar.ru/analytics/reports/2212/ (дата обращения: 12.04.2022).

7. Дарья Чебакова. Портрет типичного нарушителя служебной дисциплины. / Компания РБК. – 2021. – URL: https://www.rbc.ru/technology_and_media/26/05/2021/60aceff59a7947750b54bec7 (дата обращения: 24.03.2022).

8. Алексенцев, А.И. Понятие и структура угроз защищаемой информации // Безопасность информационных технологий. – 2000. – № 3. – С. 10–17.

9. Safa N. S., Maple C., Watson T., Von Solms R. Motivation and opportunity based model to reduce information security insider threats in organizations // Journal of Information Security and Applications. – 2018. – Vol. 40. – P. 247-257. – ISSN 2214-2126. – URL: https://www.sciencedirect.com/science/article/pii/S2214212617302600 (дата обращения: 12.04.2022).

10. Defining organisational information security culture-Perspectives from academia and industry / A. Da Veiga, L. V. Astakhova, A. Botha, M. Herselman // Computers & Security. – 2020. – Vol. 92. – P. 101713. – DOI 10.1016/j.cose.2020.101713. – EDN QHJBSK.

11. DLP И ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ Отчёт по результатам исследования / Экспертно-аналитический центр InfoWatch. 2021. – 24 с. – URL:https://www.infowatch.ru/analytics/analitika/dlp-i-ekonomicheskaya-bezopasnost-otchyot-po-rezultatam-issledovaniya (дата обращения: 12.04.2022).

12. Schaufeli, W.B. Defining and Measuring Work Engagement: Bringing Clarity to the Concept / W.B. Schaufeli, A.B. Bakker // Work Engagement: A Handbook of Essential Theory and Research. – New York: Psychology Press. – 2010. – P. 5–24. – URL: https://psycnet.apa.org/record/2010-06187-002 (дата обращения: 10.04.2022).

13. Reilly, P. Employee Engagement: Future Focus or Fashionable Fad for Reward Management? / P. Reilly, D. Brown // World at Work Journal. – 2008. – № 17 (4). – P. 37–49.

14. Астахова, Л. В. Развитие готовности будущего выпускника вуза к организационной вовлеченности как императив современного высшего образования / Л. В. Астахова // Вестник Южно-Уральского государственного университета. Серия: Образование. Педагогические науки. – 2021. – Т. 13. – № 4. – С. 19-29. – DOI 10.14529/ped210402. – EDN EJEKBZ

15. Работа с данными ИБ систем для оценки вовлеченности сотрудников. – URL: https://www.infowatch.ru/resources/webinar/video-38245?utm_source=terrasoft&utm_medium=email&utm_campaign=email041021&bulk_email_rid=406&bpmtrackid=2&bpmreplica=0&contactId=84826d85-1296-4ae7-9269-46fd7edcde36&bulkEmailRecipientId=33e54ad0-14ba-440f-9694-5dc044eb1863 (дата обращения: 12.04.2022).

References

1. GOST R 53114-2008. Natsional'nyy standart Rossiyskoy Federatsii. Zashchita informatsii. Obespecheniye informatsionnoy bezopasnosti v organizatsii. Osnovnyye terminy i opredeleniya (utv. i vveden v deystviye Prikazom Rostekhregulirovaniya ot 18.12.2008 N 532-st). – URL: https://docs.cntd.ru/document/1200075565 (data obrashcheniya: 11.04.2022).

2. Metodicheskiy dokument. Metodika otsenki ugroz bezopasnosti informatsii. Utverzhden FSTEK Rossii 5 fevralya 2021 goda. – URL: https://docs.cntd.ru/document/607699443?section=text (data obrashcheniya: 11.04.2022).

3. Otchot ob issledovanii utechek informatsii ogranichennogo dostupa v 2021 godu / Ekspertno-analiticheskiy tsentr InfoWatch. – 2022. – 32. s. – URL: https://www.infowatch.ru/analytics/analitika/v-2021-stalo-bolshe-umyshlennykh-utechek (data obrashcheniya: 12.04.2022).

4. Issledovaniye utechek informatsii ogranichennogo dostupa v 2020 godu / Ekspertno-analiticheskiy tsentr InfoWatch. – 2021. – 30. c. – URL: https://www.infowatch.ru/analytics/analitika/issledovanie-utechek-informatsii-ogranichennogo-dostupa-v-2020-godu (data obrashcheniya: 12.04.2022).

5. Utechki dannykh organizatsiy po vine ili neostorozhnosti vnutrennego narushitelya. Sravnitel'noye issledovaniye. 2013-2019 gg. / Ekspertno-analiticheskiy tsentr InfoWatch. – 2020 – 32. c. – URL: https://www.infowatch.ru/analytics/analitika/utechki-dannykh-po-vine-vnutrennego-narushitelya-2013-2019-gg (data obrashcheniya: 12.04.2022).

6. Rostelekom-Solar. Kto on – tipovoy narushitel' v rossiyskoy organizatsii? 2018-2020 / Rostelekom-Solar. – 2021. – 12 c. – URL:https://rt-solar.ru/analytics/reports/2212/ (data obrashcheniya: 12.04.2022).

7. Dar'ya Chebakova. Portret tipichnogo narushitelya sluzhebnoy distsipliny. / Kompaniya RBK. – 2021. – URL: https://www.rbc.ru/technology_and_media/26/05/2021/60aceff59a7947750b54bec7 (data obrashcheniya: 24.03.2022).

8. Aleksentsev, A.I. Ponyatiye i struktura ugroz zashchishchayemoy informatsii // Bezopasnost' informatsionnykh tekhnologiy. – 2000. – № 3. – S. 10–17.

9. Safa N. S., Maple C., Watson T., Von Solms R. Motivation and opportunity based model to reduce information security insider threats in organizations // Journal of Information Security and Applications. – 2018. – Vol. 40. – P. 247-257. – ISSN 2214-2126. – URL: https://www.sciencedirect.com/science/article/pii/S2214212617302600 (дата обращения: 12.04.2022).

10. Defining organisational information security culture-Perspectives from academia and industry / A. Da Veiga, L. V. Astakhova, A. Botha, M. Herselman // Computers & Security. – 2020. – Vol. 92. – P. 101713. – DOI 10.1016/j.cose.2020.101713. – EDN QHJBSK.

11. DLP I EKONOMICHESKAYA BEZOPASNOST' Otchot po rezul'tatam issledovaniya / Ekspertno-analiticheskiy tsentr InfoWatch. 2021. – 24 c. – URL:https://www.infowatch.ru/analytics/analitika/dlp-i-ekonomicheskaya-bezopasnost-otchyot-po-rezultatam-issledovaniya (data obrashcheniya: 12.04.2022).

12. Schaufeli, W.B. Defining and Measuring Work Engagement: Bringing Clarity to the Concept / W.B. Schaufeli, A.B. Bakker // Work Engagement: A Handbook of Essential Theory and Research. – New York: Psychology Press. – 2010. – P. 5–24. – URL: https://psycnet.apa.org/record/2010-06187-002 (дата обращения: 10.04.2022).

13. Reilly, P. Employee Engagement: Future Focus or Fashionable Fad for Reward Management? / P. Reilly, D. Brown // World at Work Journal. – 2008. – № 17 (4). – P. 37–49.

14. Astakhova, L. V. Razvitiye gotovnosti budushchego vypusknika vuza k organizatsionnoy vovlechennosti kak imperativ sovremennogo vysshego obrazovaniya / L. V. Astakhova // Vestnik Yuzhno-Ural'skogo gosudarstvennogo universiteta. Seriya: Obrazovaniye. Pedagogicheskiye nauki. – 2021. – T. 13. – № 4. – S. 19-29. – DOI 10.14529/ped210402. – EDN EJEKBZ

15. Rabota s dannymi IB sistem dlya otsenki vovlechennosti sotrudnikov. – URL: https://www.infowatch.ru/resources/webinar/video-38245?utm_source=terrasoft&utm_medium=email&utm_

campaign=email041021&bulk_email_rid=406&bpmtrackid=2&bpmreplica=0&contactId=84826d85-1296-4ae7-9269-46fd7edcde36&bulkEmailRecipientId=33e54ad0-14ba-440f-9694-5dc044eb1863 (data obrashcheniya: 12.04.2022).

АСТАХОВА Людмила Викторовна, доктор педагогических наук, профессор, профессор кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: astakhovalv@susu.ru

ВОЛЕГОВ Никита Вячеславович, студент кафедры защиты информации, Южно-Уральский государственный университет (национальный исследовательский университет). 454080, г. Челябинск, пр. им. В.И. Ленина, 76. E-mail: volegov.2323@gmail.com

ASTAKHOVA Liudmila Victorovna, Doctor of Pedagogy, Professor, Professor of the Department of Information Security, South Ural State University (National Research University). 454080, Chelyabinsk, LeninAvenue, 76. E-mail: astakhovalv@susu.ru

VOLEGOV Nikita Vyacheslavovich, student of the Department of Information Security, South Ural State University (National Research University). 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: volegov.2323@gmail.com