УДК 004.056.5

05.00.00 Технические науки

IT ДИВЕРСИИ КОРПОРАТИВНОЙ СФЕРЕ

Параскевов Александр Владимирович
РИНЦ SPIN-код= 2792-3483
старший преподаватель кафедры компьютерных технологий и систем, *Кубанский государственный аграрный университет, Краснодар, Россия*
350044, г.Краснодар, ул.Калинина, 13
paraskevov.alexander@gmail.com

Бабенков Игорь Михайлович
студент, *НЧОУ ВО Кубанский институт информзащиты,* Краснодар, Россия
350010, г.Краснодар, ул. Зиповская, 5 лит.Б
kiiz@bk.ru

Шилович Олег Борисович
РИНЦ SPIN-код= 5938-8128
ассистент кафедры экономической теории, *Кубанский государственный технологический университет, Краснодар, Россия*
350072, г.Краснодар, ул. Московская, 2
olegrgups@mail.ru

Девять из десяти диверсий совершаются людьми, так или иначе связанными с информационными технологиями. По мнению экспертов компании InfoWatch, разработчика систем защиты конфиденциальной информации от инсайдеров, причина такой профессиональной принадлежности кроется в психологических особенностях этих служащих. Подробнее разобраться в проблеме позволят пара примеров из жизни, наиболее ярко иллюстрирующие типичные черты характера профессионалов в информационной среде. Причем если первый рассказчик не стал скрывать своего имени, то второй решил остаться неизвестным. Глубокая психологическая подоплека акта диверсии часто приводит к тому, что рассерженный служащий угрожает начальству или сослуживцам, например, по электронной почте. Иногда он даже делится своими мыслями с кем-то из коллег. Другими словами, информация о готовящейся диверсии есть не только у злоумышленника. Аналитики подсчитали, что в 31% случаев сведениями о планах диверсанта располагают другие люди. Из них 64% — коллеги, 21% — друзья, 14% — члены семьи, а еще 14% — сообщники. Также удалось установить, что 62% корпоративных диверсантов продумывают свои действия заблаговременно. В 47% случаев они совершают подготовительные действия (например, кража резервных копий конфиденциальных данных). В 27% — конструируют и проверяют механизм будущей атаки (готовят логическую бомбу в корпоративной сети, дополнительные

UDC 004.056.5

Technical sciences

IT SABOTAGE IN THE CORPORATE SPHERE

Paraskevov Alexander Vladimirovich
SPIN-code = 2792-3483
senior lecturer of Department of computer technologies and systems, *Kuban State Agrarian University, Krasnodar, Russia*
350044, Krasnodar, Kalinina st., 13
paraskevov.alexander@gmail.com

Babenkov Igor Mihajlovich
Student, *Kuban institute of information protection, Krasnodar, Russia*
350010, Krasnodar, Zipovskaja st., 5 lit.B
kiiz@bk.ru

Shilovich Oleg Borisovich
SPIN-code = 5938-8128
assistant chair of economic theory, *Kuban state technological university, Krasnodar, Russia*
350072Krasnodar, Moskovskaja st., 2
olegrgups@mail.ru

Nine out of ten acts of sabotage are committed by people one way or another associated with information technologies. According to experts at InfoWatch, developer of systems to protect confidential information from insiders, the reason for this profession lies in the psychological characteristics of these employees. Reading more will allow understanding the problem with a couple of examples from the life that most powerfully illustrate typical traits of professionals in the information environment. And, although the first teller did not hide his name, the second one decided to remain anonymous. Deep psychological background of the act of sabotage often leads to the fact that a disgruntled employee threatens boss or colleagues, for example, by e-mail. Sometimes he even shares his thoughts with someone from colleagues. In other words, not only the attacker knows the information about the upcoming sabotage. Analysts estimate that other people know 31% of information about the plans of a saboteur. Of these, 64% are colleagues, 21% with friends 14% — family members and another 14% were accomplices. It was also determined that 62% of corporate saboteurs think through their actions beforehand. In 47% of cases, they commit preparatory acts (e.g., theft of confidential data backups). 27% — design and test of the future mechanism of the attack (preparing a logic bomb on the corporate network, additional hidden system entries, etc). In 37% of cases the activity of employees can be noted: of this amount, 67% of preparatory actions visible online 11% offline and 22% both

скрытые входы в систему и т. д). При этом в 37% случаев активность сотрудников можно заметить: из этого количества 67% подготовительных действий заметны в режиме online, 11% — offline, 22% — обоих сразу

Ключевые слова: IT ДИВЕРСИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, КОРПОРАТИВНАЯ СРЕДА, СЕТЕВЫЕ ТЕХНОЛОГИИ

Keywords: IT SABOTAGE, INFORMATION SECURITY, ENTERPRISE ENVIRONMENT, NETWORK TECHNOLOGY

На данный момент никто не застрахован от IT-диверсий в корпоративной среде. Вполне вероятен тот факт, что сотрудник может уничтожить стратегически важную информацию, выдать конфиденциальные сведения и т. п. Очевидно, что ущерб в этом случае может варьироваться от испорченного рабочего климата до прямых многомиллионных потерь.

Сегодня высшим исполнительным лицам и специалистам по IT-безопасности необходимо знать, как выглядит, какими мотивами руководствуется и на что способен типичный злоумышленник. Для борьбы с диверсантами «в белых воротничках» руководство обязано располагать целым арсеналом приемов. В противном случае последствия информационных диверсий станут непредсказуемыми, малоуправляемыми и эффективность всей организации будет поставлена под сомнение. Все эти вопросы как раз и являются объектом рассмотрения данной статьи.

Прежде чем переходить к аналитическим выкладкам, необходимо ответить на вопрос: что же все-таки называется корпоративной диверсией. Важность этого определения усиливается еще и тем, что диверсия — лишь часть внутренних угроз IT-безопасности, поэтому при дальнейшем рассмотрении следует различать диверсантов и, например, инсайдеров, «сливающих» конфиденциальную информацию конкурентам.

Корпоративная диверсия — это вредительские по отношению к предприятию действия, совершенные инсайдерами в силу уязвленного самолюбия, желания отомстить, ярости и любых других эмоциональных

причин. Заметим, что под емким термином «инсайдер» понимаются как уволенные, так и штатные сотрудники предприятия, а также служащие-контрактники. Корпоративные диверсии в основном совершаются из эмоциональных, и зачастую отнюдь нерациональных побуждений. Диверсант никогда не руководствуется желанием заработать, не преследует финансовую выгоду. Этим, собственно, диверсия и отличается от других инсайдерских угроз. Традиционно считается, что результатом корпоративной диверсии очень редко бывают финансовые потери. Однако последние исследования опровергают такую точку зрения, что показано на рисунке 1.

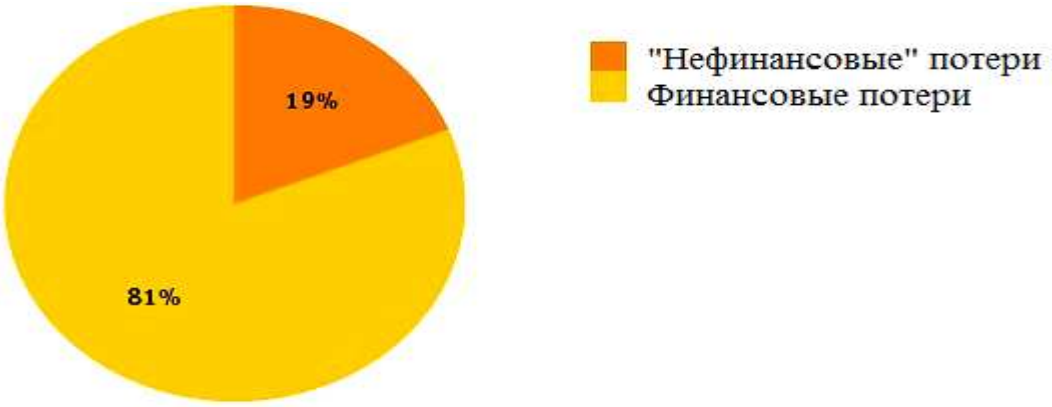

Рисунок 1 - Соотношение репутационных и финансовых потерь вследствие корпоративного саботажа

Тем не менее, на рисунке 2 показано, что суммарные финансовые потери индустрии вследствие диверсии на фоне ущерба от других внутренних и внешних угроз выглядят не очень большими.

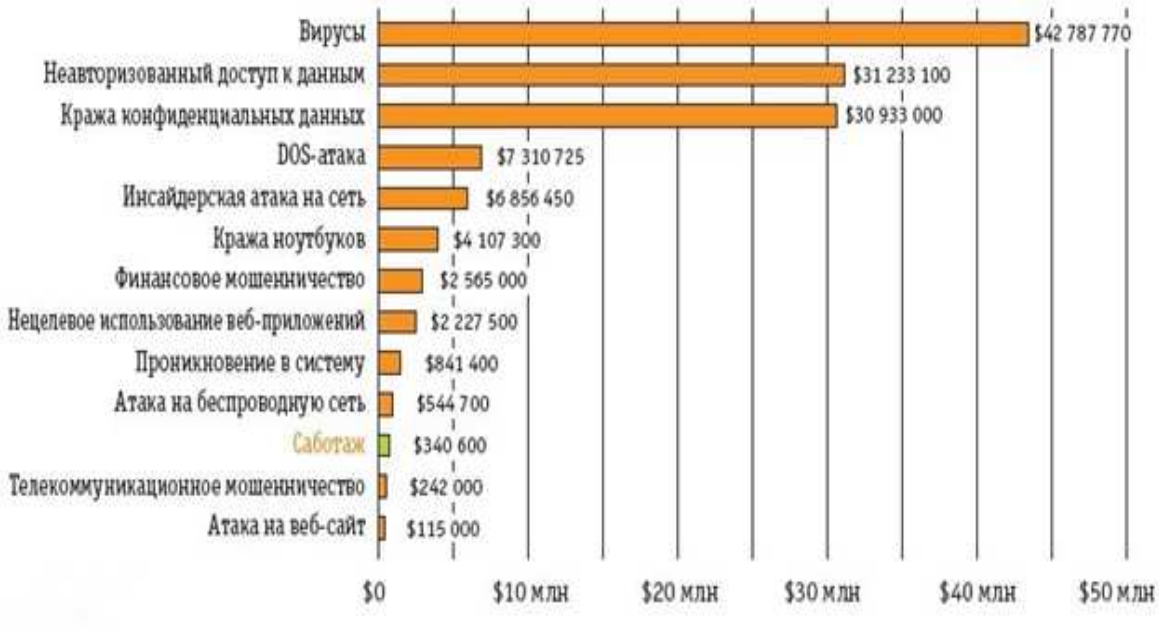

Рисунок 2 - Объем потерь от различных видов атак

Однако, интерпретация эти данных требует осторожности и известной степени внимания. Во-первых, саботаж относится к преступлениям скрытым (латентным). Респонденты очень неохотно признаются, что в их компании была корпоративная диверсия, так как это почти всегда связано с ошибками, непрофессионализмом или невнимательностью менеджмента организации. Во-вторых, диверсия действительно встречается намного реже, чем другие инциденты, поэтому суммарный ущерб получается небольшим.

Для оценки финансового ущерба вследствие диверсии воспользуемся результатами исследований CERT - центр реагирования на компьютерные инциденты (рисунок 3).

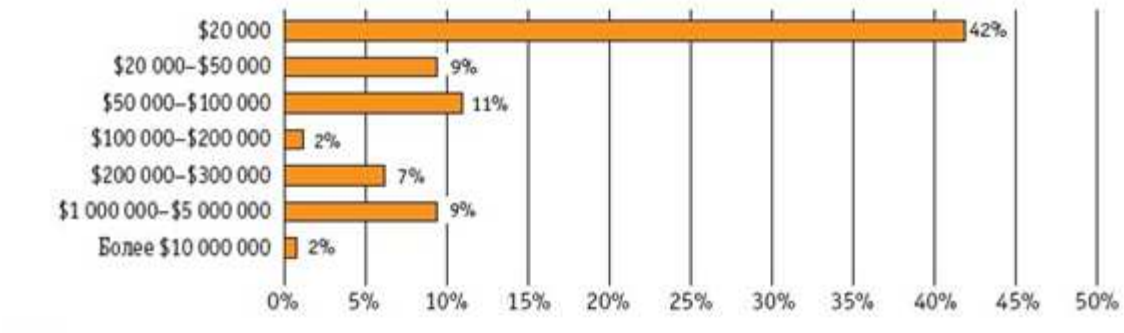

Рисунок 3 - Финансовые потери, по причине внутренней диверсии

Оставшиеся неуказанными процентные доли финансовых потерь являются несущественными. Заметим, что чуть меньше половины всех респондентов, ставших жертвами, понесли «незначительный» урон — до $20 тыс. По сравнению со средним ущербом в результате утечки конфиденциальной информации в $255 тыс. это действительно небольшие значения. Однако, наибольшую озабоченность экспертов вызывает именно та одна десятая часть, которая приходится на потери свыше $1 млн (9% — от $1 млн до $5 млн и 2% — более $10 млн). Это лишний раз указывает на некоторую относительность статистики, где суммарный ущерб за год оценен лишь в $341 тыс.

Если отвлечься от нематериальных факторов, опасность корпоративных диверсий состоит именно в гигантских, многомиллионных убытках, которые может понести абсолютно любая корпорация, окажись в ее штате человек с неустойчивой психикой. В некоторых случаях это может представлять угрозу национальной безопасности (представьте саботажника на ядерной электростанции), но в среде бизнеса, помимо финансовых потерь, возникает еще целый ряд отрицательных последствий. Во-первых, потеря репутации (выше приводился пример прямого взаимодействия диверсанта с клиентами фирмы). Во-вторых, вред, нанесенный другим служащим предприятия (выше приводился случай, когда саботажник запугал своего коллегу). Исследования показывают, что

негативные последствия для бывших коллег диверсанта встречаются довольно часто (рисунок 4).

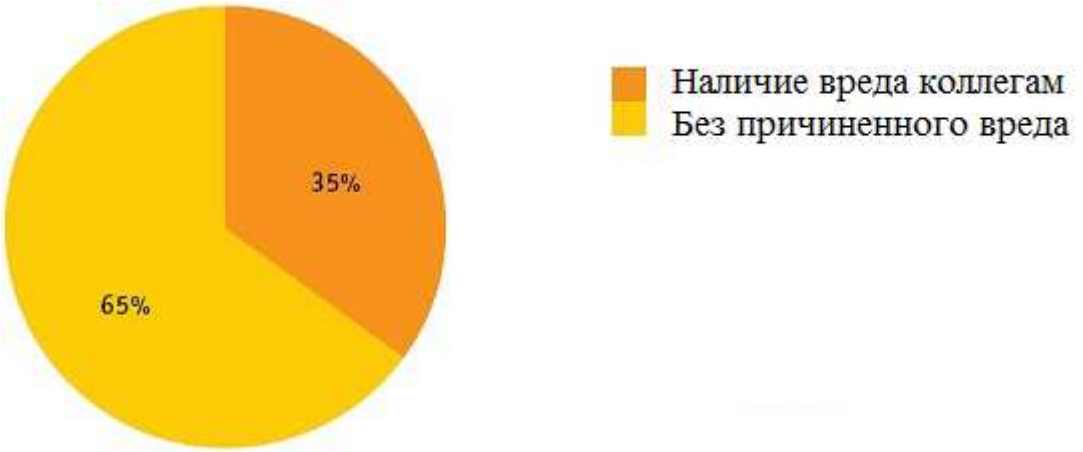

Рисунок 4 - Последствия саботажа для коллег диверсанта

Итак, диверсия может нанести огромный финансовый и моральный вред предприятию. Именно поэтому с ним необходимо бороться.

Исследование США установило, что в 98% случаев диверсантом является мужчина. Правда, портрет корпоративного саботажника не включает таких характеристик, как семейный статус, возраст и расовая принадлежность. Другими словами, это может быть как женатый мужчина, так и холостой, как 17-летний юнец, так и уходящий на пенсию служащий. Не подтвердилось также популярное убеждение, что большинство саботажников — это люди, имеющие криминальное прошлое (привлекавшиеся к ответственности, будь то административная или уголовная). Лишь в 30% исследованных случаев диверсант был хотя бы раз арестован.

Тем не менее, можно проследить мотивы, которыми руководствуются саботажники, все они носят эмоциональный характер. Более того, аналитики выяснили, что ни один диверсант не руководствовался мыслью о наживе. Однако эти мотивы представляют

собой следствия более ранних событий, которые вывели служащего из состояния морального и эмоционального равновесия (рисунок 5).

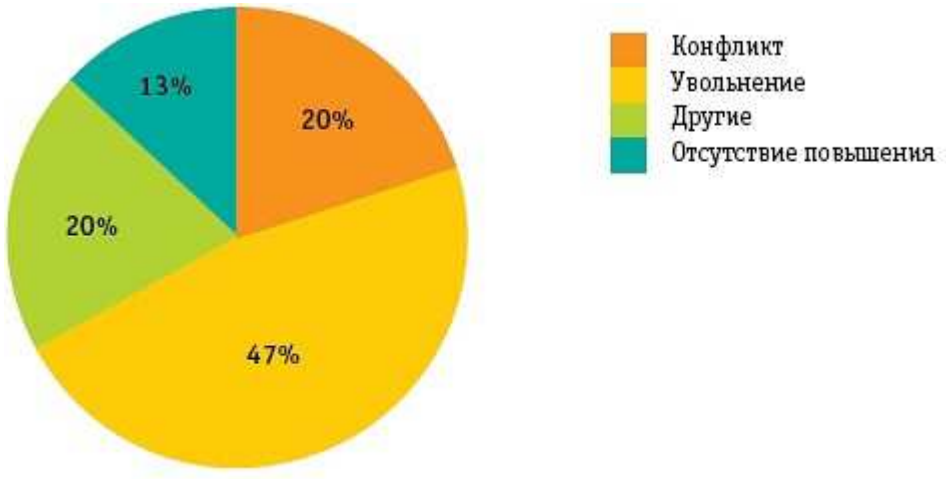

Рисунок 5 – События, предшествующие диверсии

По сведениям аналитиков, в 92% случаев диверсии предшествует неприятный инцидент на работе или целая серия таких инцидентов. В 47% случаев — увольнение, в 20% — спор с нынешними/ бывшими коллегами, 13% — отсутствие мотивации (повышения по службе, индексации зарплаты). Другими словами, 85% всех внутренних диверсантов рассержены на кого-то, кого они ассоциируют с компанией. Так, в 57% случаев сослуживцы саботажника характеризовали его как чрезвычайно рассерженного и раздраженного человека.

Многие злоумышленники на момент совершения преступления являются уже бывшими сотрудниками корпорации, сохранившими доступ к ее информационным ресурсам по каким-то причинам

Все-таки, несмотря на все эти сведения, более или менее различимая черта портрета типичного саботажника (помимо пола) — его профессия (рисунок 6).

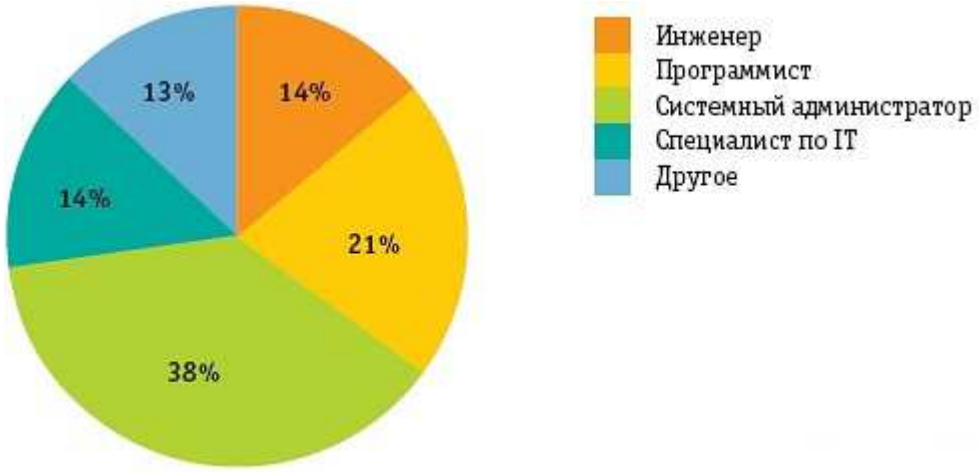

Рисунок 6 - Портрет типичного саботажника

Как показало исследование центра реагирования на компьютерные инциденты, практически все корпоративные диверсанты являются специалистами, так или иначе связанными с информационными технологиями. На долю технически подкованных диверсантов приходится 86% инцидентов. Среди них 38% системных администраторов, 21% программистов, 14% инженеров, 14% других специалистов по IT. Что же касается саботажников, не работающих в технических департаментах: 10% работают среди прочего редакторами, менеджерами, аудиторами и т. д., а 3% саботажников приходится на сферу обслуживания, в частности, на общение с клиентами.

Таким образом, из наиболее достоверных черт саботажника можно выделить всего две: это мужчина, сотрудник технического сектора.

Следует также учесть, что подавляющее большинство атак производится в нерабочее время с помощью удаленного доступа к корпоративной среде. Таким образом, даже если уволить системного администратора и сразу же заблокировать его учетную запись, но забыть о его привилегии удаленного доступа и оставить прежним пароль в системе, то рассерженный служащий сможет очень быстро отомстить начальству. В

одном из подобных инцидентов диверсанту удалось вывести из строя всю корпоративную сеть на 3 дня.

Таким образом, 57% злоумышленников имеют права администратора в системе, из них 85% на момент совершения диверсии лишились таких широких полномочий на доступ к информационной системе.

Что касается самой атаки, то 61% диверсантов предпочитают простые и незамысловатые механизмы, к примеру, команды пользователя, обмен информацией, эксплуатацию физических уязвимостей системы безопасности. Оставшиеся 39% применяют более изощренные методы атаки: собственные программы или сценарии, автономные агенты и т. д. В 60% случаев злоумышленники компрометируют учетные записи, чтобы потом с их помощью провести атаку.

В 33% инцидентов это нескрытное хранение имени пользователя и пароля; в 20% — неавторизованное создание новой учетной записи. Подчеркнем, что в 92% случаев заметить подозрительную активность в данной сфере до момента совершения диверсии не представляется возможным.

Способы обнаружения.

Предположим, что атака уже произошла. Следовательно, перед руководством среди прочего стоит вопрос о выявлении виновного. Практика показывает, что помочь в этом могут только журналы системных событий. Однако следует учитывать, что злоумышленник сделает все возможное и даже невозможное, чтобы скрыть свою личность, предстать кем-то другим или запутать следы. Во многих случаях диверсанта могут вычислить другие служащие, не имеющие с безопасностью IT-инфраструктуры ничего общего.

Если перевести эти данные на язык цифр, то получится, что 63% атак были замечены лишь потому, что в системе появились сильные отклонения. В 42% случаев система вышла из строя. При этом в 50%

инцидентов злоумышленника удается вычислить по журналам системных событий, в 23% — по IP-адресу, в 17% — по телефонным записям, в 5% — по имени пользователя, в 5% — путем процедур аудита. Таким образом, журналы событий являются наиболее эффективным средством.

В тех случаях, когда используются журналы системных событий, чаще всего нужно исследовать журнал событий удаленного доступа (53%). За ним с большим отставанием следуют журнал доступа к файлам (27%), журнал изменения системных файлов (10%), журналы приложений и баз данных (5%), почтовые журналы (5%). В общем, для идентификации злоумышленника используются сразу несколько журналов. Но не все так просто. В 76% инцидентов диверсанты пытаются скрыть свою личность (31%), действия (12%) или одновременно и то и другое (33%). Повторим, что саботажники могут модифицировать или удалять журналы событий, создавать скрытые входы в систему и неавторизованные учетные записи, подделывать свой IP-адрес. При этом 71% саботажей совершается сотрудниками, не связанными с обеспечением IT-безопасности.

По мнению экспертов, наилучшее средство предотвращения корпоративных диверсий — профилактические меры. Прежде всего компаниям нужно проверять рекомендации и места предыдущей работы нанимаемых служащих. Таким способом удается исключить те 30% претендентов, которые имели криминальную историю.

Еще один чрезвычайно эффективный метод — регулярные тренинги или семинары, на которых до персонала доводится информация об угрозах IT-безопасности и саботаже как таковом. При таком подходе руководство делает ставку на тех сотрудников, которые взаимодействуют с диверсантом в офисе, видят его нервозное поведение, получают угрозы в свой адрес и т. п. Все эти служащие должны знать, что о подобных инцидентах нельзя умалчивать. Напротив, о них следует тут же извещать уполномоченных лиц.

Следующий метод предполагает использование принципа минимальных привилегий и четкого разделения функций. Очевидно, что административных полномочий у обычных офисных служащих быть не должно. Также понятно, что сотрудник, отвечающий за резервные копии, не должен иметь возможности удалить данные в оригинальном источнике. Вдобавок в обязанности этого работника следует вменить информирование начальства в случае, если на резервные копии покусится какой-то другой служащий. Вообще, проблема защиты резервных копий может быть решена созданием их дубликатов. В сочетании с разделением ролей злоумышленнику будет практически невозможно удалить ценную информацию и избавиться от всех резервных копий. В связи с тем, что в компании, как правило, не так много по-настоящему критических данных, создание нескольких резервных копий представляется целесообразным.

Выводы.

Чрезвычайно важен момент эффективного управления паролями и учетными записями. Система IT-безопасности, разрешающая удаленный доступ уже уволенным сотрудникам, никуда не годится. Администраторы должны тщательно следить за правами доступа служащих, покидающих предприятие. Соответствующие учетные записи следует аннулировать сразу же. Лучшей профилактической мерой можно назвать мониторинг, причем не только пассивный (журналы событий), но и активный (защита ценной информации). Тогда нанести реальный ущерб компании сможет лишь топ-менеджер, поскольку у остальных работников, имеющих доступ к цифровым активам фирмы, просто не будет прав на удаление ценной информации. На рынке уже есть специализированные решения для защиты данных от внутренних угроз, в том числе и от корпоративной диверсии на предприятии. Таким образом, в распоряжении современных компаний и государственных организаций есть целый ряд средств, позволяющий минимизировать риски информационных диверсий.

Список литературы

1. Развитие человеческого капитала и рост национального богатства / Н.Б. Читанава, А.Н. Мейтова, О.Б. Шилович, А.В. Параскевов // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2014. – №01(095). С. 1192 – 1203. – IDA [article ID]: 0951401069. – Режим доступа: http://ej.kubagro.ru/2014/01/pdf/69.pdf, 0,75 у.п.л.

2. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности / Скиба В.Ю., Курбатов В.А. // Издательство: Питер, 2008, 321 с., ил.

3. Параскевов А.В. Современная робототехника в России: реалии и перспективы (обзор) / А.В. Параскевов, А.В. Левченко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2014. – №10(104). С. 1641 – 1662. – IDA [article ID]: 1041410116. – Режим доступа: http://ej.kubagro.ru/2014/10/pdf/116.pdf, 1,375 у.п.л.

4. Параскевов А.В. Этапы разработки информационной системы автоматизированного распределения заявок для ФГУП ГНИВЦ МНС РФ / А.В. Параскевов, А.В. Лега // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2015. – №06(110). С. 1090 – 1107. – IDA [article ID]: 1101506072. – Режим доступа: http://ej.kubagro.ru/2015/06/pdf/72.pdf, 1,125 у.п.л.

References

1. Razvitie chelovecheskogo kapitala i rost nacional'nogo bogatstva / N.B. Chitanava, A.N. Mejtova, O.B. Shilovich, A.V. Paraskevov // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta (Nauchnyj zhurnal KubGAU) [Jelektronnyj resurs]. – Krasnodar: KubGAU, 2014. – №01(095). S. 1192 – 1203. – IDA [article ID]: 0951401069. – Rezhim dostupa: http://ej.kubagro.ru/2014/01/pdf/69.pdf, 0,75 u.p.l.

2. Skiba V.Ju., Kurbatov V.A. Rukovodstvo po zashhite ot vnutrennih ugroz informacionnoj bezopasnosti / Skiba V.Ju., Kurbatov V.A. // Izdatel'stvo: Piter, 2008, 321 s., il.

3. Paraskevov A.V. Sovremennaja robototehnika v Rossii: realii i perspektivy (obzor) / A.V. Paraskevov, A.V. Levchenko // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta (Nauchnyj zhurnal KubGAU) [Jelektronnyj resurs]. – Krasnodar: KubGAU, 2014. – №10(104). S. 1641 – 1662. – IDA [article ID]: 1041410116. – Rezhim dostupa: http://ej.kubagro.ru/2014/10/pdf/116.pdf, 1,375 u.p.l.

4. Paraskevov A.V. Jetapy razrabotki informacionnoj sistemy avtomatizirovannogo raspredelenija zajavok dlja FGUP GNIVC MNS RF / A.V. Paraskevov, A.V. Lega // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta (Nauchnyj zhurnal KubGAU) [Jelektronnyj resurs]. – Krasnodar: KubGAU, 2015. – №06(110). S. 1090 – 1107. – IDA [article ID]: 1101506072. – Rezhim dostupa: http://ej.kubagro.ru/2015/06/pdf/72.pdf, 1,125 u.p.l.