DOI: 10.47026/2499-9636-2020-3-48-57

УДК 343.9
ББК Х515

Ю.А. КУЗЬМИН

# КРАЖА ПЕРСОНАЛЬНЫХ ДАННЫХ (криминологический аспект)

***Ключевые слова:*** *преступление, преступность, кража, хищение, персональные данные, способы защиты персональных данных.*

*Актуализируется проблема незаконного противоправного получения персональных данных. Данное преступление связано с «присвоением личности» другого физического лица с целью получения, как правило, личной выгоды. Персональные данные, на которые посягает преступник, могут представлять собой различного рода информацию. Обоснована актуальность вопросов, связанных с совершением наиболее распространенных способов хищения персональных данных. Актуальность темы вызвана тем, что кража персональных данных становится все более масштабной проблемой во всем мире, преступники изобретают все больше и больше способов получения информации, необходимой для кражи персональных данных, которые они используют с целью совершения разных преступлений. В результате использования преступниками персональных данных жертвы последствия для нее могут быть весьма серьезными. Похищенные личные данные жертвы создают анонимность для преступников и террористов и представляют угрозу как для национальной безопасности, так и для частных лиц. Проблема предупреждения краж персональных данных заключается в том, чтобы свести к минимуму возможность похищения злоумышленниками личных данных, предотвратить их незаконное изъятие. Здесь важно помнить об элементарных мерах предосторожности и безопасности. Анализируются различные способы предупреждения незаконного противоправного изъятия персональных данных.*

В наши дни утечка персональных данных кажется повседневным явлением. Кража личных данных – особый вид мошенничества, предполагающий использование чужих персональных данных для кражи денег или получения других выгод. Кража персональных данных и учетных записей сегодня является едва ли не самой распространенной компьютерной угрозой.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[1]. Кража персональных данных представляет собой преступное деяние, связанное с «присвоением личности» другого лица с целью получения кредита, кредитных карт в банках или магазинах, кражи денег с существующих счетов этого лица, подачи заявок на кредиты на имя этого лица, создания счетов в коммунальных компаниях, аренды автомобилей, подачи заявок на банкротство или даже получение работы. Во всех случаях такое хищение считается преступлением «белых воротничков».

Один из важнейших вопросов – каким образом личную информацию можно похитить [1. С. 26]. Кража персональных данных редко связана с за-

[1] О персональных данных: Фед. закон от 27.07.2006 г. № 152-ФЗ (в ред. от 24.04.2020 г. № 123-ФЗ) [Электронный ресурс] // КонсультантПлюс: справ.-прав. система. URL: http://www.consultant.ru/document/cons_doc_LAW_61801.

хватом личного имущества жертвы, однако при этом лицо, совершившее преступление, берет личную информацию жертвы, а затем использует ее противоправным образом для своей личной выгоды. Результатом этого является то, что воры личных данных могут набрать на большие суммы денег штрафы или обязательства на ваше имя. Сегодня, когда в обществе достигнут значительный технический прогресс, преступнику легче украсть номер социального страхования, номер банковского счета или любую другую информацию, которая может помочь преступнику получить доступ к личным финансам. Похитители личных данных могут получить жизненно важную информацию различными способами. Они могут просмотреть ваш мусор дома или на работе и получить сброшенный счет, почтовое письмо или кредитное заявление.

Кража личных данных может начаться, когда кто-то получит и неправильно использует такие ваши личные данные, как ваше имя и номер счета социального страхования, номера кредитных карт или другую информацию о финансовом счете. Приведем наиболее распространенные способы хищения персональных данных.

Фишинг – мошенник обманывает вас при передаче вашей личной информации. Притворяясь финансовым учреждением или какой-либо компанией, преступник отправляет на вашу электронную почту сообщения или всплывающие окна, чтобы вы могли раскрыть вашу личную информацию.

Взлом – мошенник получает доступ к вашей информации, используя слабые места безопасности на вашем компьютере, мобильном устройстве или сети.

Скримминг – кража номеров кредитных/дебетовых карт происходит с помощью специального устройства на банкоматах или при оформлении онлайн покупок.

Мошенники с удаленным доступом – мошенник обманывает вас в предоставлении доступа к компьютеру и оплате услуги, которая вам не нужна.

Отслеживание последовательности нажатия клавиш — вирусные программы, которые позволяют автоматически записывать всю печатающуюся информацию.

Подбор пароля через несколько комбинаций подбора или с помощью использования специального алгоритма.

Вредоносные компьютерные программы и программы-вымогатели – вредоносное программное обеспечение, которое позволяет мошенникам получать доступ к вашим файлам и отслеживать ваши действия, в то время как программы-вымогатели требуют оплаты, чтобы разблокировать ваш компьютер или файлы.

Фейковые онлайн-профили – мошенник устанавливает фейковый профиль в социальных сетях или на сайте знакомств и отправляет вам запрос в «друзья».

Кража документов – мошенник получает доступ к вашей частной информации через разблокированные почтовые ящики или сброшенные личные документы, такие как коммунальные платежи, продление страхования или медицинские записи.

«Притворство» – притворяются вами, когда они звонят от вашего имени финансовым учреждениям, телефонным компаниям и другим источникам, чтобы получить дополнительную личную информацию относительно вас.

Перенаправление почты – заполнение формы изменения адреса для отправки выписок по счету на выбранный адрес

«Старомодное» воровство – выхватывание платежей, почтовых отправлений (включая выписки по банковским и кредитным картам), заранее утвержденных кредитных предложений, новых чеков или налоговой информации. Жулики могут даже украсть записи отдела кадров компании или привлечь сотрудников, имеющих доступ к вашей информации.

«Дайвинг-мусорка» – программа, которая через «мусор» ищет счета или другую почту с вашей личной информацией на нем.

«Серфинг на плечах» – в общественных местах преступники могут наблюдать за вами, когда вы набираете номер и пароль своей кредитной карты, или прослушивать разговор, если вы диктуете номер своей кредитной карты по телефону.

Получение по почте заявки на «предварительно одобренные» кредитные карты, но отказываетесь от них, не уничтожая прилагаемые материалы. Преступники могут получить их и попытаться активировать карты без вашего ведома. Кроме того, если ваша почта доставляется в место, где другие люди имеют к ней доступ, преступники могут просто перехватить и перенаправить вашу почту в другое место.

Ответы на «спам» (нежелательную электронную почту), которая обещает вам некоторую выгоду, но запрашивает идентификационные данные, Как правило, заявитель не намерен выполнять свои обещания.

«Клонирование» идентичности для сокрытия. При таком виде эксплуатации вор представляется кем-то другим, чтобы скрыться от правоохранителей или кредиторов. Поскольку этот тип не является явно финансово мотивированным, его сложнее отследить, и зачастую нет бумажного следа для правоохранительных органов.

«Комбинированное» хищение идентификационных данных. В этом типе эксплуатации вор частично или полностью «изготавливает» идентичность, комбинируя различные части личной информации из разных источников. Например, вор может скомбинировать один украденный номер социального страхования с не связанным с ним днем рождения. Обычно этот вид кражи сложно отследить, поскольку в деятельности вора записаны файлы, которые не принадлежат реальному человеку.

Персональные данные, на которые посягает преступник, могут представлять собой различного рода информацию. Например, идентификационные данные, связанные с налогами физических лиц. Похитив данные, содержащие информацию о налогообложении жертвы, преступник подает ложную налоговую декларацию в налоговую службу с использованием украденного номера социального страхования.

Хищение. При краже личных медицинских данных вор использует информацию, например, номера членов медицинской страховки, для получения медицинских услуг. Поставщик медицинского страхования потерпевшего может получить счета, которые будут отражены на счете жертвы как полученные

услуги. При хищении идентификационных данных детей номер социального страхования ребенка используется преступником для получения государственных пособий, открытия банковских счетов и других услуг.

Не следует терять бдительность, необходимо обращать внимание на «тревожные» знаки, например, когда: вы получаете сообщение по электронной почте, текст или телефонный звонок с просьбой ввести или подтвердить ваши персональные данные, нажав на ссылку или открыв вложение; если сообщение содержит грамматические ошибки и плохо написано; на компьютере или мобильном устройстве имеются непредвиденные всплывающие окна с запросом на разрешение запуска программного обеспечения; получаете запрос друга от того, кого не знаете в социальных сетях; не можете войти в свою учетную запись в социальных сетях или электронной почте, либо ваш профиль вошел в систему из необычного места или с чужого компьютера; замечаете, что пропадают деньги с вашего банковского счета без каких-либо объяснений; отказано в финансовой услуге или заявка на кредит или кредитную карту отклонена, хотя вы ничего подобного не просили; получаете счета или квитанции, адресованные вам для товаров или услуг, которые не покупали.

Чтобы свести к минимуму возможность похищения злоумышленниками персональных данных, предотвратить их незаконное изъятие, важно помнить об элементарных мерах безопасности, которые необходимо взять за правило, а именно:

– не носите карту социального страхования в кошельке;

– не делитесь личной информацией (дата рождения, номер социального страхования или номер банковского счета) без особой надобности;

– проверяйте электронную почту каждый день;

– обратите внимание на подсказку по циклам выставления счетов. Если счета или финансовые отчеты просрочены, обратитесь к отправителю;

– используйте подсказки функций безопасности на мобильном телефоне;

– обновляйте всплывающие подсказки параметров общего доступа и брандмауэра при работе с всплывающей подсказкой общедоступной сети Wi-Fi. Используйте подсказку виртуальной частной сети, если вы используете открытый Wi-Fi;

– проверяйте выписку по счету кредитной карты и банковского счета. Сравнивайте поступления с выписками по счету. Следите за несанкционированными операциями;

– уничтожайте квитанции, кредитные предложения, выписки по счету и просроченным кредитным картам;

– хранить личную информацию в безопасном месте;

– установите брандмауэры и подсказки программного обеспечения для обнаружения вирусов на домашний компьютер;

– создавайте сложные пароли, которые не смогут угадать злоумышленники. Изменяйте пароли в случае нарушения своих баз данных компанией, с которой вы работаете;

– просматривайте подсказки к кредитным отчетам один раз в год. Убедитесь, что они не содержат счета, которые вы не открывали;

– «замораживайте» ваши кредитные файлы – это не позволит кому-либо подать заявку и получить разрешение на кредитный счет или коммунальные услуги на ваше имя;

– не открывайте подозрительные тексты или электронные письма, а сразу их удаляйте. Проверьте личность контактирующего с вами лица, позвонив непосредственно в соответствующую организацию – найдите их через независимый источник, такой как телефонная книга или онлайн-поиск;

– не используйте контактные данные, указанные в отправленном вам сообщении;

– не используйте один и тот же пароль для каждой учетной записи и не делитесь им ни с кем;

– не размещайте личную информацию в социальных сетях. Преступники могут «взять» вашу личную информацию и ваши фотографии для создания фальшивой личности или совершить в отношении вас мошенничество;

– при совершении платежей через Интернет оплачивайте товары только с помощью безопасной платежной службы – ищите URL-адрес, начинающийся с «https», закрытый символ замка или поставщика услуг оплаты, например, такого как PayPal;

– установите блокировку почтового ящика, измените или уничтожьте любые документы, содержащие личную информацию, прежде чем удалять их;

– не печатайте водительские права, телефон или номер социального страхования на чеках;

– немедленно сообщите об утерянных или украденных чеках. Банк заблокирует платеж по соответствующим номерам чеков. Кроме того, посмотрите новые чеки, чтобы убедиться, что никто из них не был похищен в пути;

– храните новые и отмененные чеки в безопасном месте;

– немедленно сообщите нам о любых подозрительных запросах по телефону, например о том, что звонящие запрашивают информацию о вашем счете, чтобы они могли «подтвердить заявление» или «присудить приз»;

– сохраняйте личные идентификационные номера (PIN-коды) банкоматов и кредитных карт в безопасности и не пишите PIN-код на самой карте и не храните его в том же месте, где вы обычно храните свою карту;

– уничтожайте квитанции кредитной карты, прежде чем их выбросить. Воры могут использовать их для доступа к вашим учетным записям;

– если вы получаете финансовые предложения по обычной, а не по электронной почте, которые вам не интересны, уничтожьте их, прежде чем выбросить, чтобы воры не могли использовать их для кражи ваших персональных данных. Уничтожьте любые другие финансовые бумажные документы, такие как банковские выписки или счета-фактуры, прежде чем избавиться от них.

Что могут сделать похитители с вашими персональными данными? Как только мошенник завладеет вашей личной информацией, он может делать с ней все, что захочет. Наиболее распространенными является финансовое мошенничество, например банковское мошенничество, мошенничество с кредитными картами, налоговыми льготами, выплатой пособий и мошенничест-

во в сфере телекоммуникаций. Воры личных данных могут использовать их при совершении таких преступлений, как незаконный въезд в страну или выезд из страны, незаконный оборот наркотиков и психотропных веществ, совершение киберпреступлений, отмывание денег и многих других.

В результате использования преступниками персональных данных жертвы последствия для нее могут быть весьма серьезными. Если преступник использовал личные данные другого человека для совершения преступления, это может поставить последнего под подозрение полиции. Жертва может оказаться под следствием, а в некоторых случаях бывает весьма трудно доказать свою невиновность.

Люди, которые являются жертвами финансового мошенничества, также могут столкнуться с множеством проблем. Если человек использует ваши данные в любой форме денежной транзакции, вы можете оказаться в огромных долгах. Если жертва сможет доказать, что долги не являются ее ответственностью, она не будете нести за них ответственность, однако может быть очень трудно доказать, что она не виновата. Даже если жертве удастся снять с себя ответственность за долги, удаление неверной информации из вашей кредитной истории может быть еще сложнее.

Хотя кредитные организации должны удалять неверную информацию, они часто делают это очень медленно. К тому времени, когда информация будет исправлена, возможно, уже были отклонения по ряду кредитных возможностей. Любой, кто будет проверять кредитоспособность жертвы в будущем, увидит эти отклонения, и это может повлиять на кредитные одобрения. Будет трудно получить ипотеку, новую кредитную карту или кредит. Большинство кредитных организаций помещают уведомление о внесении исправлений в кредитные файлы, но специалисты, проводящие быструю проверку кредитоспособности, могут этого не заметить. Поэтому важно как можно раньше обнаружить кражу персональных данных [3. С. 69].

Хотя кража личных данных является серьезным преступлением, жертвам редко причиняют физический вред, если только кража не произошла в результате ограбления или подобного физического воздействия на потерпевшего. Способы хищения персональных данных быстро совершенствуются по мере развития новых сред (например, социальные сети), поэтому практически невозможно полностью предотвратить кражу личных данных, однако можно снизить вероятность стать жертвой при соблюдении определенных мер предосторожности. Следует позаботиться о защите своих данных, правильно настроить параметры конфиденциальности в социальных сетях; быть в курсе подозрительных электронных писем, которые могут быть фишингом для данных; полностью уничтожать все документы, содержащие личные данные, а не просто выбрасывать их вместе с мусором.

Похищенные личные данные жертвы создают анонимность для преступников и террористов и представляют угрозу как для национальной безопасности, так и для частных лиц [4. С. 437]. Сегодня кража личных данных не является чем-то новым. Преступники и раньше подделывали удостоверения личности и платежные документы. Но сегодня угроза становится все более

распространенной, а мошенничество более изощренным, чем когда-либо, включая элементы онлайн. Правоохранительные органы используют свои киберресурсы, а также разведывательные возможности для выявления и пресечения преступных групп на ранних стадиях, а также для выявления многих типов преступников [2. С. 70]. Наряду с именами и фамилиями, номерами социального страхования и датами рождения мошенники также используют номера, адреса, свидетельства о рождении, свидетельства о смерти, номера паспортов, номера финансовых счетов (т.е. банковский счет, кредитную карту), пароли (например, девичью фамилию матери, отчество отца, кличка домашнего животного, секретное кодовое слово), номера телефонов и биометрические данные (например, отпечатки пальцев, сканирование радужной оболочки) для совершения кражи личных данных.

Отечественное законодательство в области защиты персональных данных главным образом базируется на Конституции России, международных договорах, Федеральном законе «О персональных данных» и других определяющих случаи и особенности обработки персональных данных федеральных законах. Лица, признанные виновными в нарушении прав граждан на защиту персональных данных, несут предусмотренную административным и уголовным законодательством России ответственность. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, правил обработки персональных данных, должен быть возмещен независимо от возмещения имущественного вреда и понесенных субъектом личных убытков[1].

Противоправное разглашение персональных данных имеет объектом посягательства охраняемые законом общественные отношения по обеспечению права на неприкосновенность частной жизни [5. С. 121]. Разглашение персональных данных подлежит наказанию по ч. 1 и 2 ст. 137 Уголовного кодекса РФ (далее – УК РФ) только при условии, что такие сведения соответствуют описанию предмета преступного деяния, а именно – представляют собой сведения о частной жизни либо относятся к семейной или личной тайне. Кроме того, в целях гражданско-правовой охраны частной жизни ст. 152.1 Гражданского кодекса РФ устанавливает, что информацией о ней являются сведения о личной и семейной жизни человека, его месте пребывания, жительства и происхождении. Понятия «личная тайна» и «семейная тайна» являются оценочными. Под личной тайной понимается любой факт биографии лица, который он не желает обнародовать (состояние здоровья, род деятельности, материальное положение и т.д.). Семейная тайна отличается от тайны личной по кругу носителей (сведения о внутрисемейных отношениях, образе жизни семьи и т.д.). В ч. 3 ст. 137 УК РФ установлена уголовная ответственность за незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, указывающей на личность несо-

[1] О персональных данных: Фед. закон от 27.07.2006 г. № 152-ФЗ (в ред. от 24.04.2020 г. № 123-ФЗ).

вершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего или психическое расстройство несовершеннолетнего, или иные тяжкие последствия.

Когда хищение совершается путем незаконного проникновения в электронную почту, вскрытия почтовых (бумажных) конвертов с личной перепиской и т.д., необходимо применять ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений». Действия похитителей могут не содержать состава преступления, но могут нарушать требования Федерального закона № 152-ФЗ. Их действия дают возможность утечки чужой персональной информации, а потому также наказываются, но только в рамках административного законодательства. Административная ответственность за нарушение порядка сбора, хранения, использования, распространения сведений предусмотрена ст. 13.11 Кодекса Российской Федерации об административных правонарушениях.

В США действуют два закона, которые в значительной степени определяют судебное разбирательство в связи с кражей личных данных: Закон о краже личных данных и допущении сдерживания (1998) и Закон об усилении наказания за кражу личных данных (2004). Закон 1998 г. о хищении личных данных и предполагаемом сдерживании запрещает сознательную передачу или использование средств идентификации с целью совершения, оказания помощи или подстрекательства к любой незаконной деятельности, которая представляет собой нарушение федерального законодательства или является преступлением в соответствии с применимым законодательством любого штата или местного законодательства. Кроме того, этот закон в различной степени увеличил срок наказания как за общие преступления, так и за преступления, связанные с терроризмом, и установил наказание за кражу личных данных при отягчающих обстоятельствах. Кража личных данных при отягчающих обстоятельствах означает использование личных данных другого лица для совершения уголовных преступлений. Наказание за кражу личных данных является широким и относительно суровым. Виды наказания за кражу личных данных довольно разнообразны и различаются в зависимости от степени тяжести. Виновные в краже личных данных редко избегают тюремного заключения, но при определенных обстоятельствах первого преступления преступники могут быть приговорены к испытательному сроку, если они не причинили значительного вреда. Лица, находящиеся на испытательном сроке, по-прежнему будут нести ответственность за штрафы и реституцию. Похититель может быть обязан возместить жертве финансовые потери, которые могут включать в себя потерянную зарплату, судебные сборы и даже расходы, связанные с моральным ущербом. Лиц, совершивших кражу личных данных в США, часто отправляют в тюрьму, причем минимальный срок наказания составляет два года за кражу личных данных при отягчающих обстоятельствах. Это наказание увеличивается с учетом тяжести преступного деяния.

Как и любая жертва преступления, потерпевший от хищения персональных данных претерпевает моральные страдания. Даже если вы принимаете все воз-

можные меры предосторожности, кража личных данных может произойти. Это стрессовый опыт, но от него можно оправиться. Восстановится после кражи персональных данных не просто, и в зависимости от того, что и сколько было украдено, как это произошло, может быть несколько этапов. Первыми действиями должны стать вызов сотрудников отдела по борьбе с мошенничеством из компаний, где произошло данное мошенничество, и замораживание ими ваших счетов. Затем следует включить предупреждения о мошенничестве в кредитный отчет. Следует обратиться в одно из кредитных учреждений, для этого требуется связаться также и с другими организациями. Оповещения о мошенничестве бесплатны и усложняют преступникам открытие новых счетов на ваше имя. Каждое финансово-кредитное учреждение направит вам письмо, подтверждающее, что в вашем файле размещено предупреждение о мошенничестве [6. С. 105].

Если у вас украли бумажник или он пропал, аннулируйте карты и лицензии и сообщите о паспортах и карточках социального страхования соответствующим учреждениям. Вы должны договориться с каждым ведомством о замене этих документов. Кроме того, необходимо изменить имена входа, пароли и PIN-коды.

Один из самых надежных способов защиты персональных данных, который доступен каждому, – оставаться бдительным. Следите за своими счетами. Проверяйте банковские счета и выписки по кредитным картам на предмет несанкционированных или странных покупок. Во многих банках имеются предупреждения о мошенничестве, которые можно активировать для кредитных или дебетовых карт. Другой способ предотвратить кражу личных данных – отказаться от нежелательной почты.

Кража личных данных становится все более распространенной проблемой во всем мире, мошенники находят все больше и больше способов получить информацию, необходимую для кражи личных данных. И если преступники смогли сделать это один раз, они могут сделать это неоднократно, используя каждый новый счет в качестве ориентира для следующего.

Литература

1. *Доля А.* Инциденты внутренней ИТ-безопасности: итоги года // Информационная безопасность. 2007. № 2. С. 26–29. URL: www.itsec.ru/articles2/research/incidenti_vnutrennei_it-bezopasnosti (дата обращения: 01.06.2020).

2. *Загородников С.Н., Шмелев А.А.* Основы информационного права. М.: Академический Проект, 2016. 192 с.

3. *Касаев И.Х.* Этнический аспект в компьютерной преступности // Информационная безопасность и компьютерные технологии в деятельности правоохранительных органов. 2010. № 8. С. 67–71.

4. Криминология / под ред. В.Н. Кудрявцева и В.Е. Эминова. 5-е изд., перераб. и доп. М.: Юристъ, 2014. 800 с.

5. *Кураков Л.П., Смирнов С.Н.* Информация как объект правовой защиты. М.: Гелиос, 1999. 239 с.

6. *Новиков В.К.* Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения. М.: Горячая линия-Телеком, 2015. 178 с.

**КУЗЬМИН ЮРИЙ АНАТОЛЬЕВИЧ – старший преподаватель кафедры уголовно-правовых дисциплин, Чувашский государственный университет, Россия, Чебоксары (kya70@mail.ru).**

Yuriy A. KUZMIN

**IDENTITY THEFT (Criminological Aspect)**

***Key words:*** *crime, criminality, theft, fraud, personal data, methods for protecting personal data.*

*The problem of illegal unlawful personal data obtaining is updated. The offence involves the "appropriation of identity" of another individual most commonly for the purpose of personal gain. Personal data that the perpetrator encroaches on may represent various kinds of information. The relevance of issues related to committing the most common methods of identity theft is substantiated. The urgency of the research is caused by the fact that identity theft is becoming an increasing problem around the world; criminals are inventing more and more ways to obtain the information needed to steal personal data that they use for the purpose of committing different crimes. As a result of the perpetrators' use of personal data, the consequences for the victim can be very serious. The victim's stolen identity creates anonymity for criminals and terrorists and poses a threat to both the national security and for private individuals. The problem of preventing identity theft is to minimize the possibility of personal data stealing by lawbreakers, to prevent their illegal seizure. Here, it is important to remember elementary security and safety considerations. Various ways of preventing illegal unlawful seizure of personal data are analyzed.*

References

1. Dolya A. *Intsidentyi vnutrenney IT-bezopasnosti: itogi goda* [Incidents of internal IT security: results of the year]. *Informatsionnaya bezopasnost*, 2007, no. 2, pp. 26–29. Available at: www.itsec.ru/articles2/research/incidenti_vnutrennei_it-bezopasnosti.

2. Zagorodnikov S.N., Shmelev A.A. *Osnovyi informatsionnogo prava* [Fundamentals of Information Law]. Moscow, Akademicheskiy Proekt Publ., 2016, 192 p.

3. Kasaev I.H. *Etnicheskiy aspekt v kompyuternoy prestupnosti* [Ethnic aspect in computer crime]. *Informatsionnaya bezopasnost i kompyuternyie tehnologii v deyatelnosti pravoohranitelnyih organov*, 2010, no. 8, pp. 67–71.

4. Kudryavtsev V.N., Eminov V.E., eds. *Kriminologiya. 5-e izd., pererab. i dop.* [Criminology: textbook. 5th ed.]. Moscow, Yurist Publ., 2014, 800 p.

5. Kurakov L.P., Smirnov S.N. *Informatsiya kak ob'ekt pravovoy zaschityi* [Information as an object of legal protection]. Moscow, Gelios Publ., 1999, 239 p.

6. Novikov V.K. *Organizatsionno-pravovyie osnovyi informatsionnoy bezopasnosti (zaschityi informatsii). Yuridicheskaya otvetstvennost za pravonarusheniya. Uchebnoe posobie* [The legal framework of information security (information security). Legal liability for offenses. Tutorial]. Moscow, Goryachaya liniya-Telekom Publ., 2015, 178 p.

**YURIY A. KUZMIN – Senior Lecturer of Criminal Law Department, Chuvash State University, Russia, Cheboksary (kya70@mail.ru).**