ДОРОЖНАЯ КАРТА ПРОВАЙДЕРА СЕТЕВОЙ БЕЗОПАСНОСТИ УКРАИНЫ

ROOT LEVEL RESOURCES

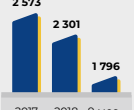
Обеспечение сетевой безопасности в Украине является одной из самых важных функций государства, поскольку благосостояние нации зависит от информационной составляющей. На сегодняшний день состояние криминогенной ситуации требует разработки и внедрения мероприятий для предотвращения преступных посягательств на объекты в сфере использования электронно-вычислительных машин (далее – «ЭВМ»), автоматизированных систем, компьютерных сетей или сетей электросвязи.

По причине социально-экономических проблем, Украина существенно отстает в развитии от стран-участниц Конвенции про киберпреступность. Кибервойны, кибертерроризм, кибершпионаж стали обыденными, поэтому преступность в информационной сфере является угрозой национальной безопасности Украины.

На сегодняшний день официальная государственная статистика содержится:

- В ведомостях про совершенные уголовные преступления, предусмотренные разделом XVI Уголовного кодекса Украины (далее – «УК Украины»), которые отображаются в отчетах Генеральной прокуратуры Украины;
- В статистической отчетности Национальной полиции Украины, где кроме уголовных преступлений, предусмотренных разделом XVI УК Украины, отображаются и другие преступления, связанные с использованием ЭВМ.

Так, согласно данным Генеральной прокуратуры Украины, зарегистрированный массив уголовных преступлений предусмотренных Разделом XVI УК Украины имеет следующие показатели за последние годы:

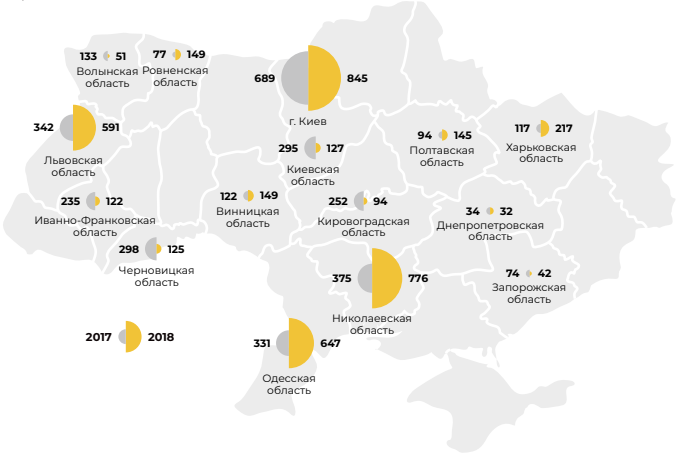


Статья УК Украины	2017	2018	9 мес. 2019
361 – Несанкционированное вмешательство в работу ЭВМ (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи.	1 795	1 023	1 014
361¹ – Создание с целью использования, распространения или сбыта вредных программных или технических средств, а также их распространение или сбыт.	35	134	165
361² – Несанкционированные сбыт или распространение информации с ограниченным доступом, которая сохраняется в ЭВМ (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации.	64	52	33
362 – Несанкционированные действия с информацией, которая обрабатывается в ЭВМ (компьютерах), автоматизированных системах, компьютерных сетях или сохраняется на носителях такой информации, совершенные лицом, которое имеет доступ к ней.	670	1 070	576
363 – Нарушение правил эксплуатации ЭВМ (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи или порядка или правил защиты информации, которая в них обрабатывается.	6	12	4
363¹ – Препятствование работе ЭВМ (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи путем массового распространения сообщений электросвязи.	3	10	4
Из них совершено женщинами:	24	84	39

В соответствии с данными Департамента киберполиции Украины, зарегистрированный массив уголовных преступлений, совершенных с использованием высоких информационных технологий выглядит следующим образом:

Статья УК Украины	2018	9 мес. 2019
176 – Нарушение авторского права и смежных прав	29	59
185 – Кража	860	767
ч. 3,4 ст. 190 – Мошенничество	2 798	1 598
200 – Незаконные действия с документами на перевод, платежными карточками и иными средствами доступа к банковским счетам, электронными деньгами, оборудованием для их изготовления	311	364
229 – Незаконное использование знака для товаров и услуг, фирменного наименования, квалифицированного указания происхождения товара	10	24
231 – Незаконный сбор с целью использования или использование сведений, составляющих коммерческую или банковскую тайну	58	218
ч. 3, 4 и 5 ст. 301 – Ввоз, изготовление, сбыт и распространение порнографических предметов	463	597
361 – Несанкционированное вмешательство в работу ЭВМ (компьютеров), автоматизированных систем, компьютерные сетей или сетей электросвязи	1 618	1 108
361¹ – Создание с целью использования, распространения или сбыта вредных программных или технических средств, а также их распространение или сбыт	28	142
361² – Несанкционированные сбыт или распространение информации с ограниченным доступом, которая сохраняется в ЭВМ (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации	57	49
362 – Несанкционированные действия с информацией, которая обрабатывается в ЭВМ (компьютерах), автоматизированных системах, компьютерных сетях или сохраняется на носителях такой информации, совершенные лицом, которое имеет доступ к ней	729	1 049
363 – Нарушение правил эксплуатации ЭВМ (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи или порядка или правил защиты инфомации, которая в них обрабатывается	11	15
363¹ – Препятствование работе ЭВМ (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи путем массового распространения сообщений электросвязи	2	11

Вот так выглядит карта Украины по количеству уголовных преступлений, совершенных с использованием информационных технологий:

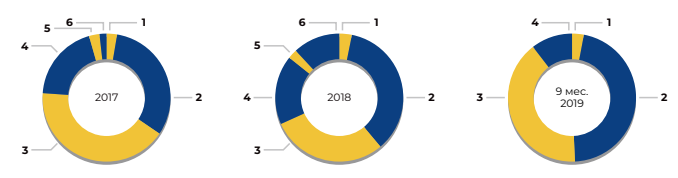


Субъекты киберпреступлений. Кого стоит опасаться?

ROOT LEVEL RESOURCES

Согласно данным Генеральной прокуратуры Украины и Департамента киберполиции Украины: **99,9% преступлений** в сфере использования ЭВМ, автоматизированных систем, компьютерных сетей или сетей электросвязи совершаются гражданами Украины.

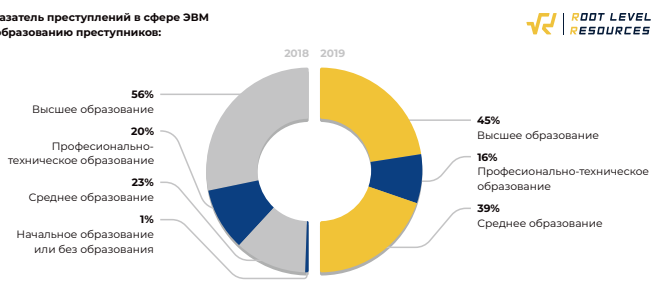
Возрастной показатель преступлений в сфере ЭВМ:



	2017	2018	9 мес. 2019
1	От 16 до 17 лет – 3%	От 16 до 17 лет – 3%	От 16 до 17 лет – 3%
2	От 18 до 28 лет – 32%	От 18 до 28 лет – 36%	От 18 до 28 лет – 46%
3	От 29 до 39 лет – 41%	От 29 до 39 лет – 29%	От 29 до 39 лет – 40%
4	От 40 до 54 лет – 19%	От 40 до 54 лет – 18%	От 40 до 54 лет – 11%
5	От 55 до 59 лет – 3%	От 55 до 59 лет – 2%	
6	От 60 лет и более – 2%	От 60 лет и более – 12%	

Показатель преступлений в сфере ЭВМ по образованию преступников:

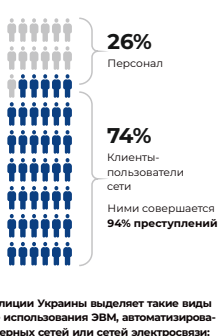
ROOT LEVEL RESOURCES



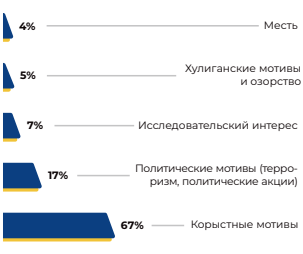
В профессионально-квалификационном плане, круг преступлений в сфере использования ЭВМ, автоматизированных систем, компьютерных сетей или сетей электросвязи невероятно широкий: коммерческие директора, банковские служащие, финансисты, программисты, инженеры и монтажники компьютерного оборудования, бухгалтеры и так далее.

Экспертами установлено, что 26% преступлений в сфере использования ЭВМ, автоматизированных систем, компьютерных сетей или сетей электросвязи совершаются руководителями организаций. Так, современные руководители, как правило, специалисты высокого уровня, владеют достаточной компьютерной подготовкой и профессиональными знаниями, имеют доступ к информации широкого круга и могут отдавать распоряжения, и при этом непосредственно не отвечать за работу компьютерной системы.

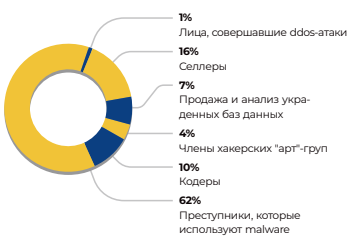
Опрошенные представители служб безопасности организаций выделяют следующую классификацию субъектов преступлений в сфере использования ЭВМ, автоматизированных систем, компьютерных сетей или сетей электросвязи:



Мотивы совершения преступлений в сфере использования ЭВМ, автоматизированных систем, компьютерных сетей или сетей электросвязи:



Департамент киберполиции Украины выделяет такие виды преступников в сфере использования ЭВМ, автоматизированных систем, компьютерных сетей или сетей электросвязи:



Что поставлено на карту?

ROOT LEVEL RESOURCES

Основными объектами, которые требуют сетевой безопасности в Украине являются:

Коммуникационные системы всех форм собственности, в которых обрабатываются национальные информационные ресурсы и/или которые используются в интересах органов государственной власти, органов местного самоуправления, правоохранительных органах и военных формированиях.

Коммуникационные системы, которые используются для удовлетворения общественных потребностей и/или реализации правоотношений в сфере электронного управления, электронных государственных услуг, электронной коммерции, электронного документооборота.

Объекты критической информационной инфраструктуры.

Основными видами преступлений в сфере использования ЭВМ, автоматизированных систем, компьютерных сетей или сетей электросвязи в Украине являются:

Сфера пользования платежными системами

1. Скиминг (шиминг) – незаконное копирование содержимого треком магнитной дуги (чипов) банковских карт.

2. Кеш-трепинг – кража средств из банкомата путем установки на шатер банкомата специальной сдерживающей накладки.

3. Кардинг – незаконные финансовые операции с использованием платежных карт или их реквизитов, которые не инициированы или не утверждены её владельцем.

4. Несанкционированное списание средств с банковских счетов с помощью систем дистанционного банковского обслуживания.

Сфера интеллектуальной собственности

1. Пиратство – незаконное распространение интелектуальной собственности в Интернете.

2. Кардшаринг – предоставление незаконного доступа к просмотру спутникового и кабельного ТВ.

Сфера электронной комерции и хозяйственной деятельности

1. Фишинг – выманивание у пользователей интернета их логинов и паролей к электронным кошелькам, сервисам онлайн аукционов, перевода или обмена валюты.

2. Онлайн мошенничество – завладение средствами граждан через интернет-аукционы, интернет-магазины, сайты и телекомуникационные средства связи.

Сфера информационной безопасности

1. Социальная инженерия – технология управления людьми в Интернет пространстве

2. Мальваре – создание и распространение вирусов и вредного программного обеспечения

3. Противоправный контент – контент, который пропагандирует экстремизм, терроризм, наркоманию, порнографию, культ жестокости и насилия

4. Рефайлинг – незаконная подмена телефонного трафика.

Потенциальные страхователи в Украине:

ROOT LEVEL RESOURCES

Жертвой кибератак потенциально могут стать все – от компании госсектора до онлайн-магазинов и сайтов медийных компаний. Однако особый интерес у злоумышленников вызывают:

1. Финансово-кредитные организации, особенно банки, которые широко используют информационные технологии. Несанкционированные вмешательства в деятельность систем Интернет-Клиент-Банк и Интернет-банкинга, кибекражи данных с банковских счетов и платежных карт клиентов является следствием большого количества преступлений в финансовой сфере. По данным Национального банка Украины, в 2018 году произошло 77,6 тысяч случаев мошенничества с банковскими картами, что привело к потере 163,7 млн. грн.
2. Дочерние компании с зарубежными инвестициями.
3. Предприятия, связанные с финансовыми потоками и большими объемами персональных данных (GDPR)
4. Компании, которые сотрудничают с партнерами из Европейского Союза.

Развитие внутреннего рынка киберстрахование требует усовершенствования механизма управления инновационной деятельностью страховых компаний который учитывает влияние эндогенных и экзогенных факторов и объединяет инструменты государственной поддержки диверсификации информационных продуктов страхования с рыночными. Основными проблемами государственного регулирования такого рынка является несовершенство нормативно-законодательной базы, отсутствие государственных стандартов функционирования и государственной финансовой поддержки.

Главными органами государственного регулирования страхового рынка в Украине является Национальная комиссия, которая осуществляет регулирование в сфере рынка финансовых услуг, Государственная служба финансового мониторинга Украины, Государственная аудиторская служба Украины. Развитие рынка киберстрахования требует тесного взаимодействия страховых компаний с Департаментом киберполиции, Национальной комиссией, которая осуществляет государственное регулирование в сфере связи и информатизации для объединения усилий, нацеленных на мониторинг киберугроз и противодействие киберпреступности. Важным направлением также является развитие сетевого взаимодействия национальных страховых компаний между собой и страховиками других стран с целью обмена положительным опытом в сфере страхования киберрисков.

Характерные виды киберрисков и направления киберстрахования в Украине:

ROOT LEVEL RESOURCES

Виды киберрисков	Направления киберстрахования рисков
Риск потери информации и нарушения работы систем при взломе пароля доступа или в следствии DDoS-атаки.	По своей сути относится к киберриску потери информации и нарушения работы компьютерных систем. Киберстрахование возмещает убытки на возобновление деятельности информационной технологии, например web-сайта.
Риск финансовых потерь через нарушение работы компьютерных систем.	По своей сути отвечает киберриску потери упущенной выгоды в offline-страховании. Направление страхования защищает IT-предприятия от потерь по вине киберпреступлений в случае нарушения работы компьютерных систем. Направление страхования является целесообразным для защиты online-магазинов, медиа-кинотеатров, систем треке-торрентов.
Риск финансовых потерь по регресс-искам при краже, разглашении или использовании персональной информации.	По своей сути отвечает киберриску потери от регресс-иска собственника данных при краже, разглашении и использовании киберпреступниками персональной информации. Это направление страхование возмещает убытки предприятия по регресс-иску собственника персональной информации.
Риск финансовых потерь по вымогательству при вирусном блокировании компьютерных систем.	Заключается в кибервымагательстве через принуждение к плате за разблокирование информационных систем или информации при предыдущем блокировании вирусом программ компьютеров или баз данных. Киберстрахование покрывает убытки на разблокирование информационных систем при доведении убытком и фиксации киберпреступлений для страховщика.
Риск финансовых потерь на восстановление программного обеспечения и/или информации, в результате действий киберпреступников.	Является аналогом имущественного страхования и относится к киберриску финансовых потерь при повреждении программного обеспечения и/или информации вследствие действий киберпреступников. Киберстрахование возмещает убытки на восстановление программного обеспечения и/или информации.

На сегодняшний день в Украине мало провайдеров сетевой безопасности. Это связано в первую очередь с тем, что некоторые риски сложно оценить и определить тариф. Кроме того и сами граждане не понимают, что нужно требовать от компаний, которым они предоставляют свои данные.

Киберстрахование в Украине должно стать новым видом страхования от уголовных киберрисков и угроз вмешательства в деятельность автоматизированных систем, поскольку страна находится в процессе информатизации, интенсивно внедряет информационные технологии во всех сферах общественной практики.

Обзор основ законодательства Украины, регулирующего вопросы правового обеспечения сетевой безопасности:

ROOT LEVEL RESOURCES

Конституция Украины от 28.06.1996 №254к/96-ВР:
https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

Кодифицированные нормативно-правовые акты:

- Гражданский кодекс Украины от 16.01.2003 №435-IV: https://zakon.rada.gov.ua/laws/show/435-15
- Кодекс Украины про административные правонарушения от 07.12.1984 №8073-X: https://zakon.rada.gov.ua/laws/show/80731-10 21 https://zakon.rada.gov.ua/laws/show/80732-10
- Уголовный кодекс Украины от 05.04.2001 №2341-III: https://zakon.rada.gov.ua/laws/show/2341-14
- Кодекс законов о труде Украины от 10.12.1971 №322-VIII: https://zakon.rada.gov.ua/laws/show/322-08
- Налоговый кодекс Украины от 02.12.2010 №2755- VI: https://zakon.rada.gov.ua/laws/show/2755-17

Законы Украины:

- Про авторское право и смежные права: Закон Украины от 23.12.1993 №3792-XII: https://zakon.rada.gov.ua/laws/show/3792-12
- Про государственное управление в сфере трансфера технологий от 14.09.2006: Закон Украины от 14.09.2006 №143-V: https://zakon.rada.gov.ua/laws/show/143-16
- Про ратификацию Конвенции о киберпреступности: Закон Украины от 07.09.2005 №2824-IV: https://zakon.rada.gov.ua/laws/show/2824-15
- О доступе к публичной информации: Закон Украины от 13.01.2011 №2939- VI: https://zakon.rada.gov.ua/laws/show/2939-17
- Про защиту информации в информационно-телекоммуникационных системах: Закон Украины от 05.07.1994 №80/94-ВР: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
- Про информацию: Закон Украины от 02.10.1992 №2657-XII: https://zakon.rada.gov.ua/laws/show/2657-12
- Про национальную программу информатизации: Закон Украины от 04.02.1998 №74/98-ВР: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80
- Про национальную безопасность Украины: Закон Украины от 21.06.2018 №2469-VIII: https://zakon.rada.gov.ua/laws/show/2469-19
- Про основные основы обеспечения кибербезопасности Украины: Закон Украины от 05.10.2017 №2163-VIII: https://zakon.rada.gov.ua/laws/show/2163-19
- Про платежные системы и перевод средств в Украине: Закон Украины от 05.04.2001 №2346-III: https://zakon.rada.gov.ua/laws/show/2346-14
- Про телекоммуникации: Закон Украины от 18.11.2003 №1280-IV: https://zakon.rada.gov.ua/laws/card/1280-15

Указы Президента Украины:

- О Доктрине информационной безопасности Украины: Указ Президента Украины от 08.07.2009 №514/2009: https://www.president.gov.ua/documents/472017-21374
- О Положении про порядок проведения криптографической защиты информации в Украине: Указ Президента Украины от 22.05.1998 №505/98: https://zakon.rada.gov.ua/laws/show/505/98
- О Положении про техническую защиту информации в Украине: Указ Президента Украины от 27.09.1999 №1229/99: https://zakon.rada.gov.ua/laws/show/1229/99
- Стратегия кибербезопасности Украины: Указ Президента Украины от 15.03.2016 №96/2016: https://zakon5.rada.gov.ua/laws/show/96/2016
- Стратегия национальной безопасности Украины: Указ Президента Украины от 26.05.2015 №287/2015: https://zakon.rada.gov.ua/laws/show/287/2015